Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Access Aware Routing Protocol (AARP) Towards Trust Management for Mobile Ad Hoc Networks

Dr. R. Vadivel
Assistant Professor
Department of Information Technology
School of Computer Science and Engineering
Bharathiar University
Coimbatore, India

Abstract— In this paper, Access Aware Routing Protocol (AARP) towards Trust Management problem for Mobile Ad hoc Network (MANET) is proposed. In MANET, nodes periodically move over the terrain space with transmission range. In this research work a scheme to handle trust establishment and aggregation issues are proposed. Unlike trust management in previous schemes, trust management in MANET involves neighbor trust relationship along with location and time factors. Trust relations as a trust graph is modelled in order to enhance accuracy and efficiency of trust establishment among mobile nodes. The proposed mechanism is a decentralized and self-configurable trust aggregation scheme. To evaluate the performance, the proposed scheme is implemented in NS2. Packet delivery ratio, delay and overhead are the performance metrics chosen for the comparison with the existing scheme. Simulation results proved that the proposed scheme outperforms in terms of the chosen performance metrics.

Keywords— Trust management, secured routing scheme, MANET, trust relationship, trust establishment.

I. INTRODUCTION

Mobile Ad hoc NETworks (MANET) has made remarkable progress in development of protocols, routing, packet forwarding and data gathering algorithms, and systems. In MANET, nodes carry out routing and packet-forwarding functions. Also the mobile nodes act as both terminals and routers. Each node is allowed to move freely and hence change its connections to other nodes frequently that results in a very high rate of network topology changes. The transmission power, computational ability, and available bandwidth of each node in MANET are limited.

While proposing a trust management mechanism, historical behaviors are recorded for each entity, and the said statistics are used to identify the way of entity is likely to behave in the future. The trust mechanism will motivate the mobile nodes to behave in a trustworthy manner, detect misbehaviour, and improve network performance. The topologies and mobility models are the remarkable component of the trust relationship research in MANETs. The topologies and mobility models fix the movement of mobile nodes that significantly impact the performance of the trust management protocol. Hence, it is a noteworthy thing to design proper trust scheme with respect to various mobility models which accurately represent the intended application scenarios. By this way the trust can be more accurately predicted.

A variety of mobility models has been proposed for MANETs. Some typical models include random-walk mobility model (RWMM) [2], random-direction mobility model (RDMM) [4], random-waypoint mobility model (RWPMM) [1], and realistic mobility model (RMM) [3]. RWMM and RDMM are the simplest mobility models depending on random directions and speeds. RWPMM introduces pause time between changes in destination, direction, and speed. RMM tries to simulate a more realistic environment by placing obstacles in the area.

However, most of the existing trust and reputation systems in MANET simply considered fixed position models that ignored the most important feature of mobility. A quantity of schemes accepted totally random mobility models that are not common in practice. Random mobility models engage substantial management overheads to uphold trust relationships in a completely random environment. Previous trust and reputation management systems with unrealistic mobility settings may not correctly reflect the true trust relationships in MANET.

II. LITERATURE REVIEW

The most popular reputation system is the feedback scheme used by eBay. The EigenTrust scheme proposed by Kamvar et al. presented a method to obtain a global trust value for each peer by calculating the eigenvalue from a trust ratings matrix [20]. Xiong and Liu developed a reputation-based trust framework PeerTrust [30]. Zhou and Hwang proposed the PowerTrust system for DHT-based P2P networks [19]. The group of Zhou, Hwang, and Cai has also built the GossipTrust system [20] and the Fuzzy Trust System [31]. Liang and Shi proposed a personalized trust model PET for resource sharing [27]. NICE is a trust inference scheme in distributed networks [25]. Zhao and Li proposed the concept of trust vector (TV) and a trust management scheme VectorTrust for aggregation of distributed trust scores [17], [18] and a group trust rating aggregation scheme H-Trust inspired by the H-Index technique [16].

Credence is a decentralized object reputation and ranking management system for large-scale P2P file-sharing networks [11]. The one-hop reputation protocol was designed for propagating reputation in P2P network for making service decisions [8]. A collaboration-based autonomous reputation system was proposed for Email services [13]. A new emerging research area in trust community is reputation systems in social networks [7], [30]. A comprehensive survey and overview on trust and reputation systems can be found in [5], [10], and [32]. Trust research for MANET is also an active area. Buchegger and Le Boudec proposed a reputation scheme to detect misbehaviors in MANET [21]. Their scheme was based on a modified Bayesian estimation method. Buchegger and Le Boudee also proposed a self-policing reputation mechanism [22]. The scheme utilized the local observation of nodes and leverages second hand trust information to detect misbehaving nodes. The CORE system adopted a reputation mechanism to achieve cooperation in MANET [6]. The goal of the CORE system was to prevent selfish behaviors. Sun et al. considered trust as a measure of uncertainty and presented a formal model to represent, model, and evaluate trust in MANET [33].

Ganeriwal et al. extended the trust scheme application scenario to sensor networks and built a trust framework for sensor networks [24]. Another ad hoc trust scheme was [34], where the trust confidence factor was proposed. In vehicular MANET, a privacy-preserving system was described to guarantee the trustworthiness of vehicle generated announcements [23]. A privacy-preserving system that guaranteed message trustworthiness in vehicle-to-vehicle communications was also proposed [12]. Li and Shen have recently proposed a hierarchical reputation management system for large-scale MANET [26]. In their work, reputation and price systems were combined to increase performance. A distributed hash-table approach was implemented to store the global reputation records. Other works with a relevant scope included [28], [9], [29], [32], and [15]. Compared with existing literatures in the trust and reputation system research community, our approach and experiment settings are significantly different. To study the trust relationships in MANET, our scheme focuses on high-mobility settings (with time and location factors). This paper presents a realistic application scenario with rich real-world data traces.

III. PROPOSED WORK

In MANET, each mobile node has short radio range, high mobility, and uncertain connectivity. Two nodes can communicate only when they reach each other's transmission range. When two nodes meet, they have a contact probability that they contact or start some transactions. Dissimilar to the completely random mobility, the movement pattern is quite common in real-world MANET. For instance, a bus system could be considered as a cyclic movement MANET. In a bus system, each bus visits stops in a scheduled route periodically.

A. Trustful Path Establishment (TPE)

Trustful Path Establishment (TPE) is a discrete-time stochastic control process consisting of a set of states. In each state, there are several actions in order to determine the next hop in a trust-path-finding process to choose. In a trust-path-finding process two states are available namely the current hop/state and the next hop/state. The state transition function determines the transition probabilities to the next state. A reward is also earned for each state transition. Value iteration is proposed to solve the TPE problem. Initially, for a sequence of random node states in trust path and a collection of all states in trust graph. The future states only depend on the present state and are independent of past states.

In each node state, the next state probabilities sum to 1. The trust-path-finding process is a stochastic process that all state transitions are probabilistic. The goal is to maximize the cumulative trust rating for the whole path, typically the expected product from the source node to the destination node. The solution to the TPE is denoted as a trust path π; the standard family of algorithms are allowed to calculate the policy π is the value which is the iteration process.

B. Working of the Trust Shift Function (TSF)

The trust shift function $TSF_{x,z} = TSF_{x,y} \oplus TSF_{y,z}$. The TSF needs to suit the following given function:

$$TSF_{x,y} \otimes TSF_{y,z} = \min\left(TSF_{xy}, TSF_{yz}\right) \times \sqrt{\max(TSF_{xy}, TSF_{yz})}$$

In each round of the iteration, the trust table of each node is updated by choosing an action (next hop state in a trust graph). The value iteration is concurrently executed for all nodes. It compares the new information with the old trust information and makes an alteration to the trust tables based on the new information. The trust tables associated with the nodes are iteratively updated to remain the local trust table updated. Utilizing the trust transfer function, the value iteration function is defined. In the initial stage, preset direct trust ratings are stored in local trust tables. Though, the direct trust information is limited and does not cover all potential interactions. Updates are every so often performed where nodes get back the trust table from one of their direct trust neighbors and replace existing trust ratings with updated trust ratings in local trust tables and then include relevant neighbors as the next hops. Each node is establishing a local trust table, which represents a current local view of the network. When there is a requirement to get a trust value on a remote node, trust search is initiated automatically.

IV. SIMULATION SETTINGS AND PERFORMANCE METRICS

100 mobile nodes starting from IP address 192.168.1.1 to 192.168.1.200 move in a 1000 x 1000 meter rectangular region for 100 seconds simulation time. The channel capacity of mobile nodes is set to the value 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs. It has the functionality to notify the network layer about link breakage. We assume each node moves independently with the constant mobility speed between 2 m/s.

All nodes have the different transmission range is 200 meters. The simulated traffic is Constant Bit Rate (CBR) with varying initial energy between 3 joules. The simulation settings are also represented in tabular format as shown in Table.1.

TABLE I: SIMULATION SETTINGS

No. of Nodes	200
Terrain Size	1000 X 1000 m
MAC	802.11b
Radio Transmission Range	200 meters
Simulation Time	150 seconds
Traffic Source	CBR (Constant Bit Rate)
Packet Size	512 KB
Mobility Model	Random Waypoint Model
Speed	2 m/s

V. RESULTS AND DISCUSSIONS

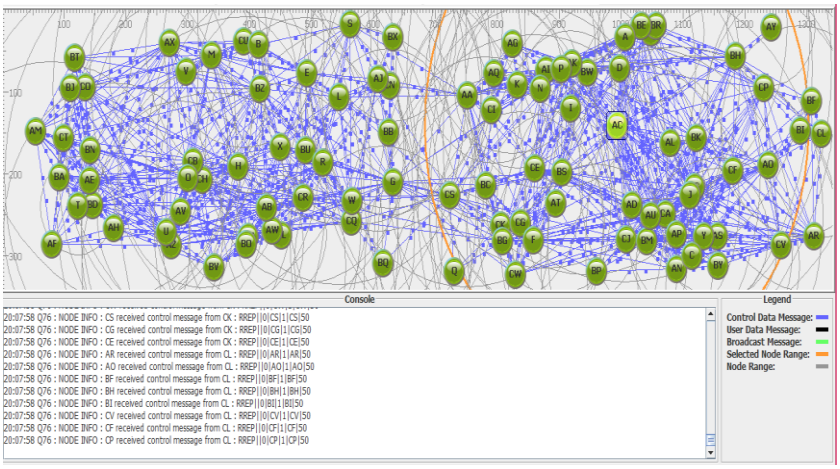

Fig. 1 NS2 Simulation

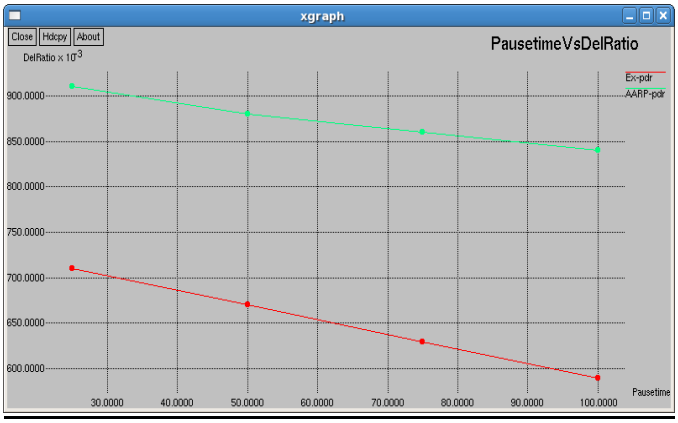

Fig. 2 Pausetime Vs Delivery Ratio

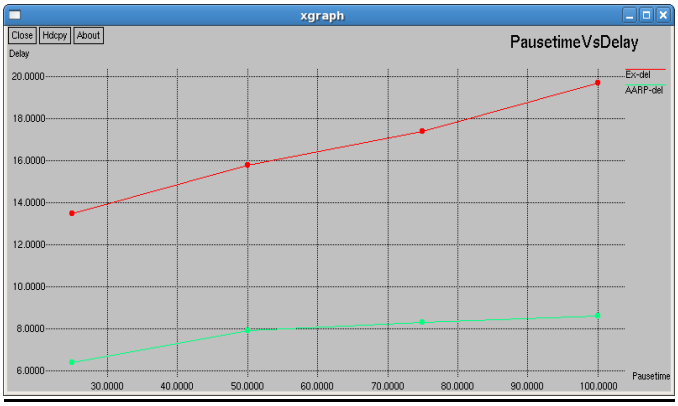

Fig. 3 Pausetime Vs Delay

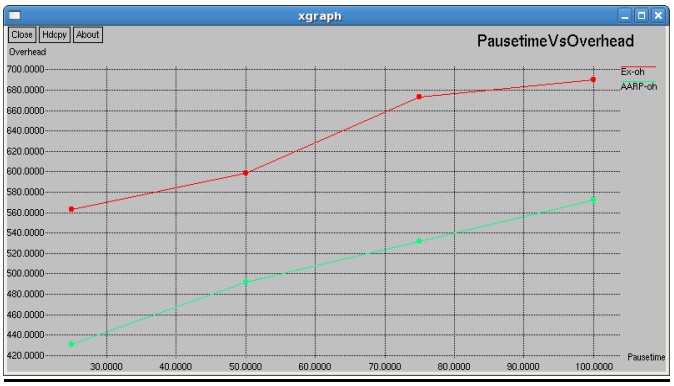

Fig. 4 Pausetime Vs Overhead

The simulations are performed using NS2 simulator as shown in the Fig. 1. From the results shown in Fig. 2, it can be clearly understood that the proposed protocol AARP attains better packet delivery ratio than that of AODV routing protocol. It is depicted in the Fig. 3 that the proposed AARP consumes comparatively lesser delay and from the Fig.4 it is to be known that the AARP consumes less overhead packets than that of AODV routing protocol.

VI. CONCLUSIONS

In this research work Access Aware Routing Protocol (AARP) towards Trust Management problem for Mobile Ad hoc Network (MANET) is proposed. It is known that in mobile ad hoc networks, nodes periodically move over the terrain space with transmission range. Hence a trust management scheme to handle trust establishment and aggregation issues are detailed. Unlike trust management in previous schemes, trust management in MANET involves neighbor trust relationship along with location and time factors. The proposed protocol which is decentralized and self-configurable nature trust aggregation scheme is employed for trust management. The proposed routing scheme is implemented using NS2 simulator tool. Packet delivery ratio, delay and overhead are the performance metrics chosen for the comparison with the existing scheme AODV. Simulation results proved that the proposed scheme outperforms in terms of the chosen performance metrics.

ACKNOWLEDGMENT

The author thank the administrative authorities of Bharathiar University to carry out this research work.

REFERENCES

[1] J. Broch, D. A. Maltz, D. Johnson, Y.-C. Hu, and J. Jetcheva, “A performance comparison of multi-hop wireless ad hoc network routing protocols,” in Proc. 4th Annu. ACM/IEEE Int. Conf. MobiCom, Dallas, TX, Oct. 1998, pp. 85–97.

[2] R. A. Guerin, “Channel occupancy time distribution in a cellular radio system,” IEEE Trans. Veh. Technol., vol. 36, no. 3, pp. 89–99, Aug. 1987.

[3] A. Jardosh, E. M. Belding-Royer, K. C. Almeroth, and S. Suri, “Towards realistic mobility models for mobile ad hoc networks,” in Proc. 9th Annu. Int. Conf. MobiCom, New York, 2003, pp. 217–229.

[4] E. M. Royer, P. M. Melliar-Smith, and L. E. Moser, “An analysis of the optimum node density for ad hoc mobile networks,” in Proc. IEEE Int. Conf. Commun., Helsinki, Finland, Jun. 2001, pp. 857–861.

[5] S. Marti and H. Garcia-Molina, “Taxonomy of trust: Categorizing P2P reputation systems,” Comput. Netw., vol. 50, no. 4, pp. 472–484, Mar. 2006.

[6] P. Michiardi and R. Molva, “Core: A collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks,” in Proc. 6th IFIP Conf. CMS, Portoroz, Slovenia, 2002, pp. 107–121.

[7] A. Mohaisen, N. Hopper, and Y. Kim, “Keep your friends close: Incorporating trust into social network-based Sybil defenses,” in Proc. 30th IEEE INFOCOM, Shanghai, China, Apr. 10–15, 2011, pp. 1943–1951.

[8] M. Piatek, T. Isdal, A. Krishnamurthy, and T. Anderson, “One hop reputations for peer to peer file sharing workloads,” in Proc. 5th USENIX Symp NSDI, 2008, pp. 1–14.

[9] A. Post, V. Shah, and A.Mislove, “Bazaar: Strengthening user reputations in online marketplaces,” in Proc. 8th USENIX Symp. NSDI, Boston, MA, Mar. 30/Apr. 1, 2011, p. 14.

[10] S. Ruohomaa, L. Kutvonen, and E. Koutrouli, “Reputation management survey,” in Proc. 2nd Int. Conf. ARES, 2007, pp. 103–111.

[11] K. Walsh and E. G. Sirer, “Experience with an object reputation system for peer-to-peer filesharing,” in Proc. 3rd Conf. Symp. NSDI, Berkeley, CA, 2006, pp. 1–14.

[12] Q.Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, “Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications,” IEEE Trans. Veh. Technol., vol. 59, no. 2, pp. 559–573, Feb. 2010.

[13] M. Xie and H. Wang, “A collaboration-based autonomous reputation system for email services,” in Proc. 29th IEEE Conf. INFOCOM, San Diego, CA, Mar. 15–19, 2010, pp. 1–9.

[14] L. Xiong and L. Liu, “PeerTrust: Supporting reputation-based trust for peer-to-peer electronic communities,” IEEE Trans. Knowl. Data Eng., vol. 16, no. 7, pp. 843–857, Jul. 2004.

[15] D. Yao, R. Tamassia, and S. Proctor, "Private distributed scalar product protocol with application to privacy-preserving computation of trust," in Proc. IFIPTM-Joint iTrust PST Conf. Privacy, Trust Manage. Security, Moncton, NB, Canada, Jul. 2007, pp. 1–16.

[16] H. Zhao and X. Li, "H-trust: A robust and lightweight group reputation system for peer-to-peer desktop grid," J. Comput. Sci. Technol., vol. 24, no. 5, pp. 833–843, 2009.

[17] H. Zhao and X. Li, "Vectortrust: The trust vector aggregation scheme for trust management in peer-to-peer networks," in Proc. 18th ICCCN, San Francisco, CA, Aug. 2–6, 2009, pp. 1–6.

[18] H. Zhao and X. Li, "Vectortrust: Trust vector aggregation scheme for trust management in peer-to-peer networks," J. Supercomput., to be published.

[19] R. Zhou and K. Hwang, "PowerTrust: A robust and scalable reputation system for trusted peer-to-peer computing," IEEE Trans. Parallel Distrib. Syst., vol. 18, no. 4, pp. 460–473, Apr. 2007.

[20] R. Zhou, K. Hwang, and M. Cai, "Gossiptrust for fast reputation aggregation in peer-to-peer networks," IEEE Trans. Knowl. Data Eng., vol. 20, no. 9, pp. 1282–1295, Sep. 2008.

[21] S. Buchegger and J.-Y. Le Boudec, "A robust reputation system for mobile ad-hoc networks," EPFL-IC-LCA, Lausanne, Switzerland, Tech. Rep. IC/2003/50, 2003.

[22] S. Buchegger and J. Y. Le Boudee, "Self-policing mobile ad hoc networks by reputation systems," IEEE Commun. Mag., vol. 43, no. 7, pp. 101–107, Jul. 2005.

[23] V. Daza, J. Domingo-Ferrer, F. Sebe, and A. Viejo, "Trustworthy privacypreserving car-generated announcements in vehicular ad hoc networks," IEEE Trans. Veh. Technol., vol. 58, no. 4, pp. 1876–1886, May 2009.

[24] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," ACM Trans. Sens. Netw., vol. 4, no. 3, pp. 1–37, May 2008.

[25] S. Lee, R. Sherwood, and B. Bhattacharjee, "Cooperative peer groups in NICE," in Proc. 22nd Annu. Joint Conf. IEEE INFOCOM, IEEE Comput. Commun. Soc., Mar./Apr. 2003, vol. 2, pp. 1272–1282.

[26] Z. Li and H. Shen, "A hierarchical account-aided reputation management system for large-scale MANETs," in Proc. 30th IEEE INFOCOM, Shanghai, China, Apr. 10–15, 2011, pp. 909–917.

[27] Z. Liang and W. Shi, "PET: A personalized trust model with reputation and risk evaluation for P2P resource sharing," in Proc. 38th Annu. HICSS, Jan. 2005, p. 201b.

[28] Z. Liang and W. Shi, "Analysis of ratings on trust inference in open environments," Perform. Eval., vol. 65, no. 2, pp. 99–128, Feb. 2008.

[29] R. A. Shaikh, H. Jameel, B. J. d Auriol, H. Lee, S. Lee, and Y.-J. Song, "Group-based trust management scheme for clustered wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 11, pp. 1698– 1712, Nov. 2009.

[30] M. Sirivianos, K. Kim, and X. Yang, "Socialfilter: Introducing social trust to collaborative spam mitigation," in Proc. 30th IEEE INFOCOM, Shanghai, China, Apr. 10–15, 2011, pp. 2300–2308.

[31] S. Song, K. Hwang, R. Zhou, and Y.-K. Kwok, "Trusted P2P transactions with fuzzy reputation aggregation," IEEE Internet Comput., vol. 9, no. 6, pp. 24–34, Nov./Dec. 2005.

[32] Y. L. Sun, Z. Han, W. Yu, and K. J. R. Liu, "A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks," in Proc. 25th IEEE INFOCOM, Barcelona, Spain, Apr. 2006, pp. 1–13.

[33] Y. L. Sun, W. Yu, Z. Han, and K. J. R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 305–317, Feb. 2006.

[34] G. Theodorakopoulos and J. Baras, "On trust models and trust evaluation metrics for ad hoc networks," IEEE J. Sel. Areas Commun., vol. 24, no. 2, pp. 318–328, Feb. 2006.

