ISSN:2320-0790

compusoft
An International Journal of Advanced Computer Technology

Selection of Trusted Nodes in MANET by using Analytic Network Process

Jayalakshmi V[1], Dr. Abdul Razak T[2]
[1]Department of Computer Applications, Sudharsan Engineering College, Tamilnadu, India
[2]Department of Computer Science, Jamal Mohamed College, Tamilnadu, India

Abstract: MANET is a set of limited range wireless nodes that function in a cooperative manner so as to increase the overall range of the network. The performance of ad hoc networks depends on the cooperative and trust nature of the distributed nodes. To enhance security in ad hoc networks, it is important to evaluate the trustworthiness of other nodes without centralized authorities. In this paper, a novel dynamic trust quantization model with multiple decision factors based on Analytic Network Process (ANP) decision theory is proposed. The multiple decision factors include direct trust, recommendation based trust, active degree, similarity degree and packet forwarding ratio. These multiple trust factors are incorporated to reflect trust relationship's complexity and uncertainty. Based on the trust factors, the selection of the trusted nodes is obtained by using Analytic Network Process. An information theoretic framework which uses ANP is presented in this paper. ANP is used for making trust decisions which replaces the Analytic Hierarchy Process (AHP) already used in the literature. The AHP reduces a multidimensional problem into a one dimensional one. Decisions are determined by a single number for the best outcome or by a vector of priorities that gives an ordering of the different possible outcomes. The selected nodes obtained by using the ANP decision theorem eliminate the malicious nodes and helps to protect the network from any internal attacks

Keywords: Trust , routing, analytic network process, MANET, security

I. INTRODUCTION

Mobile Ad Hoc Networks (MANETs) are collections of wireless mobile nodes, constructed dynamically without the use of any existing network infrastructure or centralized administration. Due to the limited transmission range of wireless network interfaces, multiple hops may be needed for one node to exchange data with another one across the network. MANETs are characterized by limited power resource, high mobility and limited bandwidth. Owing to the openness in network topology, the security of communication in ad hoc wireless networks is important, especially in military applications. The absence of central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber-attacks[1] than wired networks. These attacks are generally classified into two types: passive and active attacks. Passive attacks do not influence the functionality of a connection. An adversary aims to interfere in a network and read the transmitted information without changing it. If it is also possible for the adversary to interpret the captured data, the requirement of confidentiality is violated. It's difficult to recognize passive attacks because under such attacks the network operates normally. In general, encryption is used to combat such attacks. Active attacks aim to change or destroy the data of a transmission or attempt to influence the normal functioning of the network. Active attacks when performed from foreign networks are referred to as external attacks. If nodes from within the adhoc network are involved, the attacks are referred to as internal attacks.

In order to combat passive and active attacks, a secure ad hoc network is expected to meet the different security requirements such as Confidentiality, Integrity, availability, authentication and non-repudiation. Recently, there are many scholars contributing to the researches [2-5] on secure and trusted routing. They can be mainly classified into two categories: cryptographic technique and non-cryptographic technique. The cryptographic technique mainly focuses on traditional safety mechanisms called hard security strategy. These traditional safety mechanisms for providing confidentiality, authentication, and availability are not efficient in MANETs, where network nodes have limited communication bandwidth, CPU cycles, memory, and battery capacity. These traditional safety mechanisms come at the cost of computation complexity of encryption algorithms, memory usage for storing security information, and network bandwidth for key synchronization and certificate distribution and revocation.
In fact, the very challenge of securing distributed networks comes from the distributed nature of these network and the

wireless nodes must cooperate in order to establish communications dynamically using limited network management and administration. Collaboration is only productive if all participants operate in an honest manner. Therefore, establishing and quantifying trust, which is the driving force for collaboration, is very important for securing distributed networks. Some trust models have been proposed in the wired networks. However, they are inapplicable to the MANET due to the difference in network topology and application scenario.

In this paper, a novel trust management model is proposed to select the trusted nodes which exclude the malicious nodes in order to establish a secure communication. The multiple trust decision [7,8] evaluating factors are obtained and it includes direct trust, recommendation trust, active degree , similarity of degree and packet forwarding ratio. Based on the trust decision factors, the selection of the trusted nodes are obtained by using Analytic Network Process (ANP)[9] . The proposed model calculates the trust value of node based on the ANP. The trusted path obtained by using the ANP decision theorem eliminates the malicious nodes and helps to protect the network from any internal attacks.

The remaining paper is organized as follows. Section 2 describes the related work which gives the basic definition and metrics used in the trust and also the various trust management models proposed in the literature. In section 3 the proposed trust model is presented and it describes the various trust evaluating factors. Section 4 describes the ANP and the selection of the trusted nodes among the other nodes in the network is done and the conclusion is presented in the section 5.

II. Related work

A. Trust

A standard definition considers trust to be a measure of subjective belief that one person or party uses to assess the probability another will perform a favourable action before the opportunity presents itself to monitor whether that activity has occurred. When a person is considered trustworthy; it is meant that there is a high probability that the actions they are expected to perform will be done in a manner that is favorable to the truster .The overall measure of trust that changes through time. The measurement of the trust [10] can be levied against the measure of risk and the measure of trust may also be affected by control systems in place.

B. Trust Models

Although there has been substantial work on trust management models, their applicability in mobile agent systems has received limited research attention

Beth et al. [11] proposed a trust management model, which introduced the concept of experience to express and measure trust, in which the credibility formula was derived and integrated. This model divided 'trust' into direct trust and recommendation trust which were used to describe the trust relationship, respectively, between the subject and object, subject and recommendation object. A trust management model was proposed by Josang [12] based on the subjective logic model, which introduced the evidence space and the conception space to describe and measure the concept of trust relationships. This model defined a set of subjective logic operators for the derivation and comprehensive calculation of trust value. From the evolutionism and sociology points of view, Mui [13] first introduced a trust and reputation computing model for generalized networks. In the indirect trust evaluation process, they proposed a graph parallelization algorithm, which is intuitive and easy to understand. In the model established by Sun et al. [14, 15], trust is measured by entropy. They introduced an entropy function to represent the trust value between two nodes, which really captured the dynamic nature of trust evidence. To compute the indirect trust value, both George and Sun's models used trust value iteration techniques considering multi-level directed graph. When more nodes are involved, the convergence speed of this scheme is exponentially slow, and its flexibility becomes a big challenge. In the subjective trust evaluation model proposed in the [16] uses the credibility of nodes can be evaluated using analytic hierarchy process theory and fuzzy logic rules prediction method. The model can detect malicious nodes only if there are few in the numbers and also it utilized AHP [17] to set up a hierarchical skeleton within which multi-attribute decision problems can be structured to determine the weight for the trust factors. Yet, the strict hierarchical structure may need to be relaxed when modeling a more complicated decision problem that involves interdependencies between elements of the same cluster or different clusters.

III. Proposed Trust Model based on ANP

In ad hoc networks, every node acts as a host and a router simultaneously. As a host, the entity needs to run user's application; as a router, it needs to forward data packets according to the routing protocols. Trust is a relationship between two neighboring entities. Trust value expresses the degree that one node expects another node to offer certain services. Existing trust management models focus on how to evaluate and obtain accurate trust values, and how to use the results in trust applications. An evaluating node quantifies all relevant information about an evaluated node, including the observations on the node's behaviour, interaction records, views from other nodes, and so on. It uses an appropriate model to quantify the credibility of the evaluated node. The trust values are easily used for routing decision, which acts as a special trust application.

Definition : Adhoc network contains many nodes and these nodes are independent in nature and the network can be considered as a weighted graph $G = (V, E, Tv)$, where V is the set of all nodes, E is the set of all edges and $Tv{:}Tv(E_{ij}) \rightarrow R\varepsilon[0,1]$denotes the value of the trust of the node.There is an edge between two nodes if they are located within each other's transmission range. A path between the source node VS and the destination node VD can be represented as a node sequence *P = (VS,…..Vi ,…, VD), where* $V_i \varepsilon V$.

The trust model of an adhoc network can be represented as the weighted directed graph as in the Fig.1. Each node in the model maintains a trust table which contains the trust values of the neighbouring nodes.

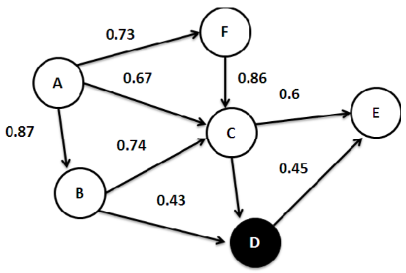

Figure 1. Weighted graph in the Adhoc Networks

A. *Trust Decision Factors*

To access a nodes trust value , literatures generally use two methods : direct or indirect . Trust between immediate neighboring nodes is known as Direct Trust and is required for cases where a trust relationship is formed between two nodes without previous interactions and the indirect trust is receiving this information second hand through the form of recommendations. From this a belief level can be calculated on the routing behaviour of this node it received from other nodes. In this proposed model to access the trust value of a node, apart from the direct and recommendation based trust, three more trust evaluating factors are used namely packet forwarding ratio, active degree and the similarity degree.

Direct Trust

Let DT_{ij} present the direct trust value from node i to node j, then DT_{ij} can be got from the history records and context information between the two nodes. A simple formula [18] can be used to calculate the direct trust factor as in equation (1).

$$DT_{\mathrm{ij}} = \rho \frac{1+\sum_{k=1}^{i} S_k}{2+\sum_{k=1}^{i} N_k} + (1-\rho)\frac{\alpha E_p + \beta C_q + \gamma M_t}{\alpha+\beta+\gamma} \quad -----(1)$$

S_k presents during the recent I times interactions, the real total service count at the kth time between node i and node j. N_k presents the expected service count of node i at the kth time. Node i often make observation at different time instances. Let S_k denote the time when node i make observation of node j. At time k, node i observes that node j performs the action times upon the request of performing the action times. Obviously, $N_k \geq S_k$. These history factors describe that the observation has been made for a period of time, and it should carry less importance than the observation made recently. E_p, C_q, M_t presents the node information at the current time. Ep is the energy consumption information, which represents the power resources as the mobile embedded system; Cq is the processor utilization percentage, which represents the calculation resources; M_t is the memory utilization percentage, which represents the storage resources. α , β and γ are all positive integers, which represents the weight values of the three aspects. $\rho \varepsilon [0,1]$, is the variable coefficient.

Recommendation Based Trust

Based on the Eigen Trust algorithm proposed by Kamvar et al. [19] which derives global reputation scores in P2P communities with the purpose of assisting members in choosing the most reputable peers, the evaluation of the recommendation based trust factor is obtained in the proposed model.

Eigen Trust assumes that each node V_i observes whether its interactions with a node V_j have been positive or negative. The satisfaction score $S_{V_i V_j}$ for node V_j as seen by node V_i is based on the number of satisfactory interactions *sat(*V_i,V_j*)* and the number of unsatisfactory interactions *unsat(*V_i,V_j*)*, and is expressed as:

$$S_{V_iV_j} = sat(Vi, V_j) - unsat(V_i, V_j)$$

The normalized local trust score C_{ij} of node V_j as seen by node V_i is computed as:

$$C_{ij} = \frac{\max(S_{V_iV_j},0)}{\sum_{l\in L}\max(S_{V_iV_l},0)} -----------(2)$$

where L is the local set of nodes with which node V_i has had direct experiences. This step effectively normalizes the local trust values to the range [0,1] and thereby removes any negative trust values. A local node with a large negative satisfaction score would thus have the same normalized local trust score as a local node with satisfaction score 0.

In Eigen Trust, trust scores of nodes one hop outside node V_i's local group, denoted by RT_{ik}, can be computed from two connected trust arcs with the following formula:

$$RT_{ik} = \sum_{j\in L} C_{ij}C_{jk} -----------(3)$$

This step effectively collapses functional trust and referral trust into a single trust type, and uses multiplication of normalized trust scores as the transitivity operator. While this allows for simple computation, it creates a potential vulnerability. A malicious node can for example behave well during transactions in order to get high normalized trust scores as seen by his local nodes, but can report its own local trust scores with false values (i.e. too high or too low). By combining good behaviour with reporting false local trust scores, a malicious agent can thus cause significant disturbance in global trust scores.

The computation of global trust scores takes place as follows. In the Eigen Trust model, C = [c_{ij}] represents the matrix of all normalized local trust values in the community, $\overrightarrow{C_i}$ represents the vector of node V_i's local trust values, and $\overrightarrow{RT_i}$ represents the vector containing the trust values $\overrightarrow{RT_{ik}}$, where node V_i and node V_k are separated by ' n' intermediate nodes (loops included). Then $\overrightarrow{RT_i}$ can be expressed

$$\overrightarrow{RT_i} = C^n \overrightarrow{c_i} ------------(4)$$

When n is large, the vector $\overrightarrow{RT_i}$ will converge to the same vector for every node V_i, which is the left principal eigenvector of C. The vector $\overrightarrow{RT_i}$ is a global trust vector in the Eigen Trust model, and quantifies the community's trust in node k.

Similarity Degree

Similarity in MANET is a subjective judgment a mobile node makes about another's owned attributes based on its preference and standpoint. Similarity indicates the relationship between user attributes. The mobile nodes having an exactly the same or similar affiliated organization may also have a stronger trust in each other than the ones with different affiliated organizations. Since trust is defined in the context of similarity conditions, the more similar the two users are the greater their established trust would be considered [20]. In order to compute the similarity between users, a variety of similarity measures have been proposed, such as Pearson correlation, cosine vector similarity, Spearman correlation, entropy-based uncertainty and mean-square difference. However, Breese et al in [21] and Herlocker et al. in [22] suggest that Pearson [23] correlation performs better than all the rest.

If we define the subset of itmes that nodes V_x and V_y have co-rated as I = {ix : x =1, 2 ...n}, γ_{v_x, i_n} as the rating of node V_x to item ix and $\overline{\gamma_{v_x}}, \overline{\gamma_{v_y}}$ as the average ratings of the node V_x and V_y r espectively, then the established trust between two nodes is defined as the Pearson Correlation [22] of their associated rows in the nodes-item matrix given in the equation.

$$ST_{x \to y} = sim(v_x, v_y) = \frac{\sum_{h=1}^{n} (\gamma_{V_x, i_h} - \gamma_{V_x})(\gamma_{V_y, i_h} - \gamma_{V_y})}{\sqrt{\sum_{h=1}^{n} (\gamma_{V_x, i_h} - \gamma_{V_x})^2} \sqrt{\sum_{h=1}^{n} (\gamma_{V_y, i_h} - \gamma_{V_y})^2}} --(5)$$

Packet Forwarding Ratio

It is the proportion of the number of packets forwarded correctly to the number of those supposed to be forwarded. Correct forwarding means a forwarding node not only transmits a packet to its next hop node but also forwards devotedly (correct modification if required). For instance, when a malicious neighbor node forwards a data packet after tampering with data, it is not considered as correct forwarding. If the sender monitors this illegal modification, the forwarding ratio of this neighbor will decrease. At time t, FR(t) is computed as follows

$$FR(t) - \frac{N_{pcketscorrectlyforwarded}}{N_{allrequestingpackets}} -----(6)$$

In mobile ad hoc networks, all packets can be classified into two types: control packets and data packets. The accuracy of control packets plays a vital role in establishment of accurate routes in the network. So FR is divided into two parts: Control packet Forwarding Ratio, denoted by CFR, and Data packet Forwarding Ratio, denoted by DFR. They are computed using forwarding count of control packets and data packets according to formula (6) respectively.Using the time stamp mechanism to analyze each interaction interval .Till to current timet, there are n intervals from time 0 (i.e., [t1, t2, ..., tn]). For the kth interaction interval, node V_i assessed node V_j's trust value via the following equation:

$$w1XCFR_{ij}(t_k) + w1XDFR_{ij}(t_k) ---------(7)$$

CFR_{ij} (tk) and DFR_{ij} (tk) represent for control packet forwarding ratio and data packet for-warding ratio, in time intervaltk, respectively.

Active Degree

This decision factor reflects the level of activity of an entity in a network. It is used to indicate the credibility of evaluated entity. If an (evaluated) entity has a higher active degree, other (evaluating) entities is willing to interact with it due to its expected higher trust level. An evaluating node v_i records the cumulative number of entities interacting with an evaluated node v_j , and calculates the active degree of the evaluated node as follows:

$$AD_{ij} = 1 - \frac{TrustThreshold}{L+1}, L \geq 0 ---------(8)$$

L represents for the cumulative number of entities interacted with the evaluated node v_j

B. *Analytic Network Process*

The Analytic Network Process is a generalization of the Analytic Hierarchy Process, by considering the dependence between the elements of the hierarchy. Many decision problems cannot be structured hierarchically because they involve the interaction and dependence of higher-level elements in a hierarchy on lower- level elements. Therefore, ANP is represented by a network, rather than a hierarchy. To make tradeoffs among the many objectives and many criteria, the judgments that are usually made in qualitative terms are expressed numerically. To do this, rather than simply assigning a score out of a person s memory that appears reasonable, one must make reciprocal pair wise comparisons in a carefully designed scientific way. The fig. 2 shows the selection of the trusted node and the node choice hierarchy by using ANP.

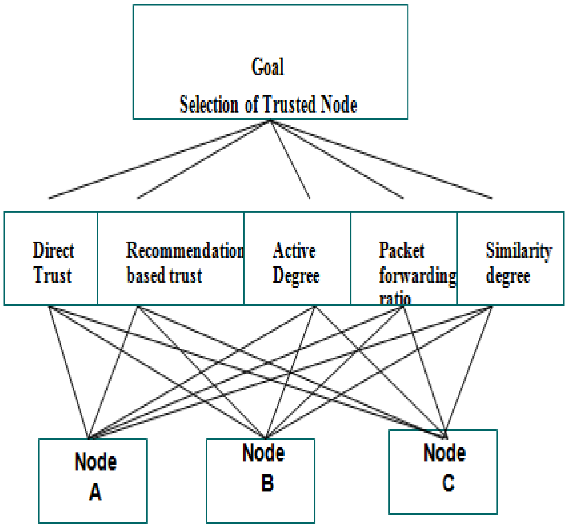

Figure 2. The Node Choice Hierarchy

According the below mentioned factors a model is developed by using ANP in trusted node selection.

- Several criteria and alternatives can be evaluated with the scope of the decision problem.
- Both objective and subjective factors can be taken into consideration in the decision problem.
- There exists an interaction between and within trusted node selection criteria and alternatives.

The proposed ANP model in trusted node selection is given in Fig. 3.

,

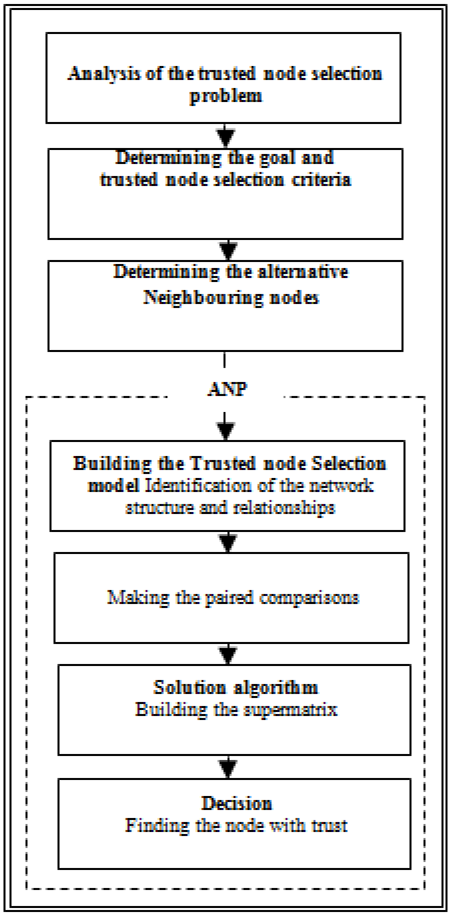
Analysis of the trusted node selection problem
Determining the goal and trusted node selection criteria
Determining the alternative Neighbouring nodes
ANP
Building the Trusted node Selection model Identification of the network structure and relationships
Making the paired comparisons
Solution algorithm
Building the supermatrix
Decision
Finding the node with trust

Figure: 3. The proposed ANP model in trusted node selection.

The proposed trust model reviews the nodes according to the evaluation criteria such as the trust evaluating factors namely direct trust, Recommendation based trust, active degree, similarity degree, packet forward ration and after this evaluation, the nodes which exceed the trust threshold value are added to the approved trusted node list of the transmission. All the packets are sent through the approved trusted nodes. The fig. 3 shows the selection of the trusted node based on the multiple trust decision factors evaluated using the formulae described in the section 3.

IV. CONCLUSION

In this paper, a novel trust management model has been proposed. The Analytic Network Process Decision Theory is used in this paper to evaluate the trustworthiness of node considering the multiple trust decision factors obtained by different methods. ANP extends the function of AHP and is a viable method for multi-criteria decision problems that involve interdependent relationships and it reduces a multidimensional problem into a one dimensional one. Decisions are determined by a single number for the best outcome or by a vector of priorities that gives an ordering of the different possible outcomes. The novel trust model presented in this paper can kick out the untrustworthy nodes and selects only the trustworthy nodes in the network so that a reliable passage delivery route is obtained. To make a further improvement for the trust prediction model proposed in this paper, we plan to incorporate other decision factors to our trust model. The problem of dynamic behavior modification will also be considered. In addition, as an application of the proposed trust model , a novel reactive routing protocol on the basis of the standard dynamic source routing, a new trusted dynamic source routing protocol will be proposed and the comprehensive performance evaluation will be conducted to compare with other routing protocols.

V. REFERENCES

[1] Kannhavong, Bounpadith, et al. "A survey of routing attacks in mobile ad hoc networks." Wireless communications, IEEE 14.5 (2007): 85-91.

[2] Y-C Hu and A. Perrig, “A Survey of Secure Wireless Ad Hoc Routing,” IEEE Sec. and Privacy, May–June 2004.

[3] K. Sanzgiri et al., “A Secure Routing Protocol for Ad Hoc Networks,” Proc. 2002 IEEE Int’l. Conf. Network Protocols, Nov. 2002

[4] Li, Xiaoqi, Michael R. Lyu, and Jiangchuan Liu. "A trust model based routing protocol for secure ad hoc networks." Aerospace Conference, 2004. Proceedings. 2004 IEEE. Vol. 2. IEEE, 2004.

[5] Ghosh, Tirthankar, Niki Pissinou, and Kami Makki. "Towards designing a trusted routing solution in mobile ad hoc networks." Mobile Networks and Applications 10.6 (2005): 985-995.

[6] Pirzada, Asad Amir, and Chris McDonald. "Trust establishment in pure ad-hoc networks." Wireless Personal Communications 37.1-2 (2006): 139-168.

[7] Xiao-Lin, LI Xiao-Yong GUI. "Trust Quantitative Model with Multiple Decision Factors in Trusted Network [J]." Chinese Journal of Computers 3 (2009): 004.

[8] Xia, Hui, et al. "A Subjective Trust Management Model with Multiple Decision Factors for MANET Based on AHP and Fuzzy Logic Rules." Proceedings of the 2011 IEEE/ACM International Conference on Green Computing and Communications. IEEE Computer Society, 2011.

[9] Saaty, Thomas L. "Analytic network process." Encyclopedia of Operations Research and Management Science. Springer US, 2001 8-35.

[10] G. Theodorakopoulos and J. S. Baras, “Trust evaluation in ad-hoc networks,” in Proceedings of the 3rd ACM workshop on Wireless security, 2004, pp. 1–10.

[11] Beth,T., Borcherding, M., Klein, B.: ‘Valuation of trust in open network’.Proc.ESORICS, 1994, pp.3–15

[12] Josang,A.:‘A logic for uncertain probabilities’ ,Int.J.Uncertainty, Fuzziness, Knowledge-Based Syst., 2001, 9,(3),pp 179–311 13

[13] Mui, L.: ‘Computational models of trust and reputation: agents,evolutionary games, and social networks’. PhDthesis, Massachusetts, 2003

[14] Sun,Y.L.,Yu,W.,Han,Z.,Ray,L.K.J.:‘Information theoretic framework of trust modeling and evaluation for ad hoc networks’, IEEE J. Sel.Areas Commun., 2006, 24, (2), pp.305–319

[15] Sun,Y.L.,Yu,W.,Han,Z.,Ray,L.K.J.:‘Trust modeling and evaluation in Adhoc networks ’.Proc. Global Telecommunications, 2005,pp.1–10

[16] Xia, Hui, et al. "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory." Wireless Sensor Systems, IET1.4 (2011): 248-266

[17] Satty, T.L.: ‘The analytic hierarchy process’ (McGraw-Hill, New York, 1980)

[18] Dai, Hongjun, Zhiping Jia, and Zhiwei Qin. "Trust Evaluation and Dynamic Routing Decision Based on Fuzzy Theory for MANETs." Journal of Software (1796217X) 4.10 (2009).

[19] S. Kamvar, M.Schlosser, and H. Garcia-Molina, “The EigenTrust Algorithmfor Reputation Management in P2PNetworks,” in Proceedingsof theTwelfthInternational WorldWideWebConference, Budapest, May2003.

[20] Ziegler, C.N. and Lausen, G. “Analyzing Correlation Between Trust and User Similarity in Online Communities”. Proc. of the 2 nd International Conference on Trust Management, 2004

[21] Breese, J. S., Heckerman, D. and Kadie, C. “Empirical analysis of predictive algorithms for collaborative filtering”. Proc. of the 14 th Conference on Uncertainty in Artificial Intelligence, 1998.

[22] Herlocker, J. L., Konstan, J. A., Borchers, A., and Riedl, J. “An Algorithmic Framework for Performing Collaborative Filtering”. Proc. of the 22nd ACM SIGIR Conference on Research and Development in Information Retrieval, 1999

[13] Pearson K. “Mathematical contribution to the theory of evolution: VII, on the correlation of characters not quantitatively measurable”. Phil. Trans. R. Soc. Lond. A, 195, 1-47, 1900.