Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

A NEW APPROACH TO TRUST EVALUATION FOR CLUSTER BASED MANETS

[1]RAJKUMAR MYLSAMY, [2]SUBRAMANIAN SANKARANARAYANAN
[1]Department of Information Technology, Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India
[2]Vice chancellor, Karpagam University, Coimbatore, Tamilnadu, India
E-mail: [1]rajkumar.mylsamy@gmail.com, [2]drsraju49@gmail.com

ABSTRACT

A Mobile Ad hoc NETwork (MANET) is a pool of independent, dynamic, wireless devices that forms a network, devoid of no permanent infrastructure. This inherent features and wireless nature of mobile ad hoc networks makes them vulnerable to a wide variety of attacks. To discover routes with trusted nodes, we propose an approach for constructing a route without malicious nodes. To forward packets through trusted nodes, this protocol evaluates various trust parameters of neighboring nodes. To prevent a node from same attack, a weight is calculated and assigned dynamically. Simulations are done using NS2 simulator. Our proposed approach has been analyzed and evaluated for performance metrics such as packet delivery ratio, control overhead, packet drop ratio, jitter and end to end delay. Dynamic weight assignment of individual trust parameters reduces end to end delay and control overhead resulting in less packet drop ratio and high packet delivery ratio. We compare our work with other clustering algorithms, which are CBTRP and 2ACK. Our analysis and simulation result clarifies that, the proposed work effectually identifies and isolates malicious nodes and it outperforms the other algorithms.

Keywords: *Mobile Ad hoc Network, Clustering, Network security, Privacy, Routing protocol*

1. INTRODUCTION

A Mobile ad hoc network is a collection of mobile nodes that self-configures to form a network without any pre-established infrastructure and centralized administration [1- 3]. Due to open working environment, MANETs are vulnerable to attacks by malicious nodes. Protocols used for routing in MANET can be classified as proactive [5], reactive [6, 7] or hybrid routing [8, 9]. In proactive routing method, every node consequently maintains the updated routing information. In reactive routing method, only when routing information is needed, routing information are created and maintained. Hybrid routing method is a combination of these proactive and reactive routing methods. To balance the performance and overhead of proactive and reactive routing methods, Hybrid routing scheme is proposed. As like hybrid routing methods, clustering methods [10, 11] are proposed to enhance the routing performance and to reduce complexity. A virtual portioning of a network into a smaller sub networks, called as clustering method. Cluster Head (CH) is a node, which is having higher stability among all the members in a cluster. Also CH maintains cluster member information and topology of respective cluster information [12]. A node that connects more than one adjacent cluster is called as gateway node [13]. Since MANETs are infrastructure less and dynamic network, to protect this network from malicious nodes are hard to achieve. Existing trust value based protocols [14-16] for Cluster based MANETs, focuses on allocating trust value to a node based on considering security factors such as packet delivery ratio, packet misrouting ratio, packet alteration ratio, and packet injection ratio as collective factor, and no weight value is assigned to the separate factors that they deliberate. Based on this observation, we proposed our approach, a new trust evaluation algorithm by considering above security factors, based on the preference value assigned to each trust parameter is proposed. The objective of our approach for trust election is to deliver a predefined trust assignment for a node for cluster based MANET. The rest of the paper is deliberated as follows: Section 2 briefly explains Literature work. In section 3, the details of our routing algorithm are presented. Section 4 shows the

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

simulation outcomes. Finally, section 5 delivers conclusion and future work of our proposed work.

2. RELATED WORK

In this section, we present related works and background information for trust selection methods used in Mobile ad hoc networks.

Several security routing algorithms [17, 18] were proposed to address security concerns of mobile ad hoc networks. These algorithms can be classified into two groups: Cryptography-based or Reputation-based security algorithms. Cryptography based security algorithms were studied in [19, 20], and these are based on mathematical theory and computer science practice. These algorithms are either symmetric-key cryptographic algorithms, in which receiver shares the same key, or Asymmetric-key cryptographic algorithms, in which two different but mathematically related keys are used. In Reputation based security algorithms [21-23], rely on reputation and trust value of a node and are not based on cryptographic method. Several trust models have been proposed for trust management. These are centralized and de-centralized algorithms [24, 25]. In centralized algorithms (CA), trust values are maintained in centralized common node and are based on positive and negative ratings. In De-centralized algorithms (DCA), a node assigns a trust value for every visited node. The work proposes a new algorithm, based on a decentralized algorithm. Many algorithms are proposed for trust identification of a node in Cluster based routing for MANET. Trust value is evaluated in [26] based on two parameters, which is a self-evaluation of trust and sum of other nodes' trust evaluation. In [27], Trust value of a node is analyzed based on average trust value given by neighboring nodes in a cluster. In [28], Trust is identified based on Behavior, Observation, and Belief (BOB) of a node during protocol execution. In CBTRP [29], Trust value of a node is identified based on Belief, Disbelief and Uncertainty identified by immediate neighbor nodes. If trust value is lesser than given threshold, then node is identified as malicious node, and such a malicious node is avoided in routing process. Thus, CBTRP proves better in identifying malicious nodes and packet transmission through malicious node is avoided. 2ACK scheme is proposed in [30]. In routing path, 2ACK scheme transmitting two hops acknowledgement packets in opposite direction. A, B, C are assumed as three consecutive nodes along the route. To guarantee in delivering a packet in node C, it sends 2ACK to node A. It detects misbehaving links rather than misbehaving nodes, which will cause the higher rate of packet drops.

3. PROPOSED WORK

The main objective of this paper is to provide security algorithms for cluster based MANET routing. This pro-posed trust model comprises three modules, Trust derivation, Trust classification and Trust computation. This model identifies malicious and non-malicious nodes in network.

3.1 Trust derivation

This module computes the trust value of a node in network. For e.g., trust value between two nodes, node 'A' and node 'B' is calculated as following. Node A takes into account individual understanding of the past transaction with another node, node B. The following diagram Figure 1 illustrates this.

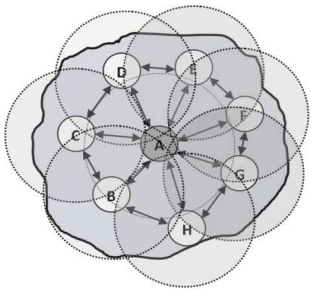

Figure 1: *Individual understanding of neighboring nodes*

3.2 Trust classification

Node's trust value is evaluated based on the following trust parameters.

1. Packet Dropping Ratio (pdr)
2. Packet Misrouting Ratio (pmr)
3. Packet Falsely injected Ratio (pfr)
4. Packet Altering Ratio (par)

Trust classification mainly based on three different values, that is High, Medium and Low values. These values are determined based on trust parameters (Packet drop ratio, Packet misrouting ratio, Packet falsely injected ratio, Packet alteration ratio).

Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 1: Trust Classification

Trust identification		Trust Classification		
		High (H)	Medium (M)	Low (L)
Trust Parameters	Pdr	$d_v<d_1$	$d_1 \le d_v \le d_2$	$d_v>d_2$
	Pmr	$m_v<m_1$	$m_1 \le m_v \le m_2$	$m_v>m_2$
	Pfr	$f_v<f_1$	$f_1 \le f_v \le f_2$	$f_v>f_2$
	Par	$a_v<a_1$	$a_1 \le a_v \le a_2$	$a_v>a_2$

The percentage result of each trust parameter is obtained, and these are stored in concerned linguistic variables d_v,m_v,f_v, and a_v. If these received values are in the range $\{d_v<d_1, m_v>m_1, f_v<f_1, a_v<a_1\}$, $\{ d_1 \le d_v \le d_2, m_1 \le m_v \le m_2, f_1 \le f_v \le f_2, a_1 \le a_v \le a_2\}$ and $\{ d_v>d_2, m_v>m_2, f_v>f_2, a_v>a_2\}$ of trust parameters pdr, pmr, pfr, and par respec-tively. Then, to determine range of values High, Medium and Low values 1, 0.5 and 0 are assigned. Trust classifi-cation is handled based on the Table 1.

3.3 Weight assignment

Result of each trust factor is assigned in its linguistic variables d_v, m_v, f_v, and a_v. Node's trust parameter value of a cluster is calculated during cluster formation process. For every node in a cluster, these values are identified for each trust parameter and then average value is calculated and stored in descending order. The maximum affected parameter is assigned with lower weight value and the least affected parameter is assigned with higher weight value. Thus, we can protect same type of attack in the network. Weight assignment calculation is represented in Table 2. From this, we can identify the weighting coefficient value for individual trust parameters.

3.4 Trust calculation

Trust value for a node is calculated based on variable value with concern weighting coefficient values $\{W_m, W_a, W_d, W_f\}$. Therefore, node A's trust on another node B is calculated as,

$$T_B^A = W_3(d_v) + W_1(m_v) + W_4(f_v) + W_2(a_v) \quad (1)$$

Where $W_1+W_2+W_3+W_4=1$. If the calculated value of node's trust is less than its relative threshold (e.g.: 0.5), then the node is assumed as malicious. Hence, it is not allowed to participate as 'Cluster member' in a network. Otherwise, if the calculated trust value of a node is greater than its relative threshold, then the node is assumed as non-malicious, and it is allowed to participate as a 'Cluster member' in a network.

3.5 Cluster formation

Initially, all nodes in network broadcast HELLO messages with node ID (MAC address). Nodes are updated in timed interval. Based on updated node list, each node in a network calculates its node value. Node value is computed based on the following parameters.

The degree difference (D_{diff}):

Degree difference is calculated as the difference between cluster size 'S' and the actual number of neighbors. It evaluates the remaining number of nodes it can handle.

$$D_{diff} = | D_{diff} | = d_i - S \quad (2)$$

Here, d_i is the degree of the node and is the threshold value for all nodes in the respective cluster

The Mobility of the node (Mob_{AB}):

Mobility of the node at time is calculated using the below formula:

$$Mob_{AB} = \frac{1}{(t_2 - t_1)} \sqrt{(p_2 - p_1)^2 + (q_2 - q_1)^2} \quad (3)$$

The remaining battery power of the node is E_A.

Therefore, Stability value of Node is calculated as $S_A = (S_1 \times D_{diff}) - (S_2 \times Mob_A) + (S_3 \times E_A)$ where S_1, S_2 and S_3 are the weight values assigned and these are in a relation such that $S_1 + S_2 + S_3 = 1$. Depending upon the Stability value of node values, the node with the highest Stability value elects itself as CH and it is updated in Neighbor table that is present in every member of cluster. Abstract data structure for construction of a cluster is called as Neighbor table and Cluster Adjacency Table (CAT) is used for holding information about the nearby clusters. In a Cluster, CAT in CH keeps the (MAC ID) IDs of the adjacent Cluster Heads; gateway node identification (MAC ID) IDs to reach adjacent Cluster Heads. Communication of CH with an adjacent cluster is handled by Gateway node.

3.6 Cluster renovation

Due to the mobility in MANET, the clusters have to be restructured and reconfigured. There may be a situation where a cluster may be

Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

reconfigured based on Stability value of cluster head (CH), node mobility, and cluster head mobility. Once TTL value of HELLO packet is 0, CH will initiate the stability factor calculation to nodes in a cluster. Each node calculates its stability value and passes it to their CH. Now CH will decide a new CH by looking at all the nodes' stability values. This information is broadcasted to all 1-hop neighbours, and it is updated in all nodes' NAT and CAT. When a node moves to another CH, it broadcasts HELLO message to neighbours in the cluster. The updated value of HELLO packet is verified by CH, and its stability value is analysed by CH. New node joins the new cluster and if necessary CH role is updated with new node. This information is broadcasted to all 1-hop neighbours.

3.7 Route discovery and route recovery

This section describes our algorithm, which uses trusted members, trusted heads, and trusted gateways to forward the packet from source to destination. In Route discovery, it first transmits a routing request (RREQ) message to its cluster head. The information present in RREQ message is needed for routing. The adjacent cluster head will receive the RREQ and checks RREQ message. It identifies whether it is destination. If a node is not actual destination, a Cluster head also verifies whether the given destination node addresses is present in its Neighbour table. If it is verified, then it forwards the RREQ message to one hop nearby neighbour, which is the destination. Upon delivering the ACK, source or CH or gateway saves the address of a next hop in its routing table. Till the destination CH receives RREQ, the searching of a next hop is repeated. Upon receiving RREQ message, actual destination is identified by verifying the address present in RREQ and NT. CH node forwards RREQ to destination. When the RREQ packet reaches CH, it verifies the next node is a trusted one or not, by verifying a trust factor less than 0.5. After assuring the next node is malicious, immediately it identifies another path to destination. Hence, the malicious node is isolated and it is protected from the routing process. Route recovery will be initiated if any route failure occurs. If a route failure is identified due to nodes' mobility in the intermediate clusters, the defined path should be reconstructed and restarted either from the local node of cluster where route failure is discovered or from the source CH.

4. SIMULATION RESULTS

4.1 Simulation parameters

Our proposed work is performed using the NS2 network simulator. IEEE 802.11 standard is used as MAC layer protocol. The radio propagation model used is the Two-Ray ground model. Nominal transmission range is 250 meters. The radio model is simulated with a nominal bit rate of 11 Mbps. The traffic type is Constant Bit Rate (CBR) with network packet rate of 4 packets/sec, and the packet size is 512 bytes. The movement model used is a Random way point model. The pause time used is 0 second. The simulation time used is 800 second. The value of High, Medium, and Low for Trust classification are 1, 0.5 and 0 respectively. The value of weights W1, W2, W3, and W4 for simulations are 0.1, 0.2, 0.3 and 0.4 respectively. The value of Weights for identifying stability factors and are 0.5 and 0.5 respectively. The value of d factors for packet delivery ratio d1 and d2 are 5% and 10%.

4.2 Packet delivery ratio

The ratio of total number of packets brought to the destination node to the total number of packets sent from the source node is defined as Packet delivery ratio. Figure 2, It shows that during transmission, intermediate nodes have several routes to the destination node so that when detecting malicious nodes, they can try an alternate route to forward packets and thus improve the packet delivery ratio. This shows that the proposed our approach can efficiently deliver the packets by detecting and isolating misbehavior nodes than CBTRP and 2ACK.

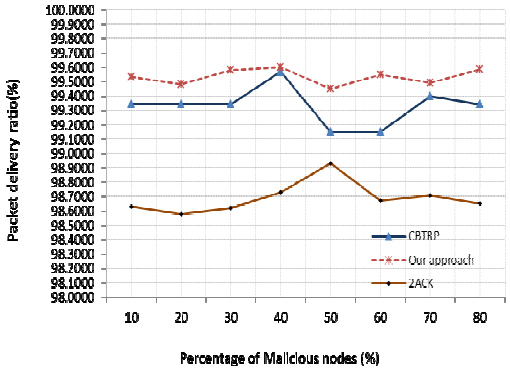

Figure 2. *Packet delivery ratio of our approach, CBTRP and 2ACK*

4.2.1 Control overhead

Journal of Theoretical and Applied Information Technology
30th June 2014. Vol. 64 No.3

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

The ratio of the number of control packets (route request, route reply, error packets, sequencing) transmitted to the number of data packets delivered is defined as Control overhead. Figure 3 show that our approach is very efficient in terms of control overhead in data delivery. The work analyses the control overhead in our approach, CBTRP and 2ACK on two conditions (with and without considering malicious nodes).

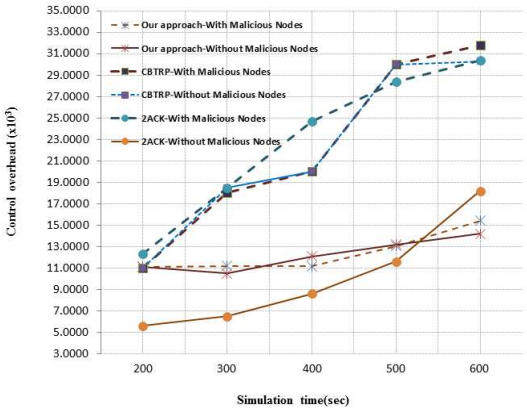

Figure 3. *Control overhead of our approach, CBTRP and 2ACK*

Control overhead of our approach is less than CBTRP and 2ACK. Our proposed approach does not do cluster head re-election process periodically for cluster maintenance.

4.3 Throughput

The percentage of misbehaving nodes versus average aggregated throughput is shown in Figure 4.

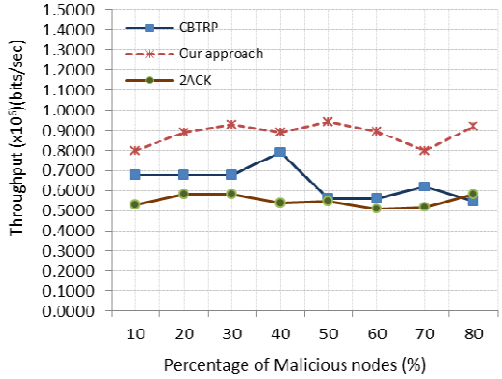

Figure 4. *Throughput average of our approach, CBTRP and 2ACK*

As a comparison, CBTRP and LEACH methods are simulated to find the relationship between percentage of misbehaving nodes and throughput. Misbehaving nodes are increased from 20% to 80% of total nodes, and the results show that the proposed method outperforms CBTRP and LEACH in terms of throughput.

4.4 Jitter

It is a measure of variability over time of packet latency across a network. A network has a jitter only if it has a variation in latency.

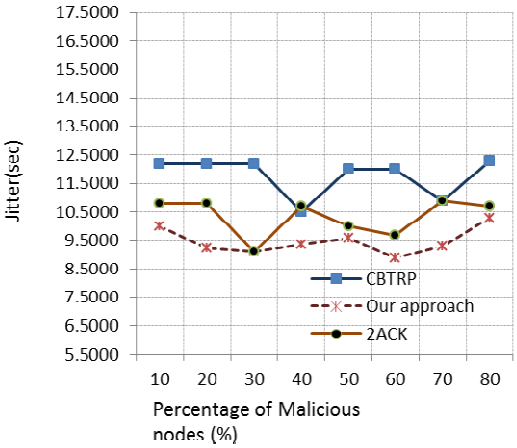

Figure 5. *Packet latency (Jitter) of 2PTH, CBTRP and 2ACK*

Jitter also called as Packet delay variation can result in both increased latency and packet loss. As Figure 5 shows, the jitter value is very low in comparison with CBTRP and LEACH. This is because of unprocessed traffic in a node. Since the proposed work considers individual trust parameters for isolating misbehaving nodes, it protects same node is affected. It is significantly less compared to others.

4.5 Packet dropping

Figure 6 shows the result of packets drop for the schemes when the number of misbehavior node is increased. From the result, we can see that our proposed work has significantly less packet drops than the CBTRP and 2ACK. This is because of our approach is immediately isolating the misbehavior nodes from trusted nodes.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

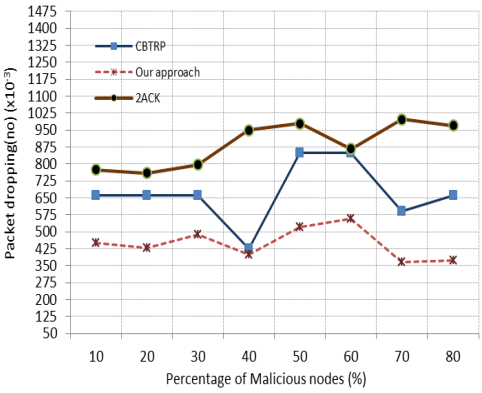

Figure 6. *Packet drop level of our approach, CBTRP and 2ACK*

5. CONCLUSION

The existence of malicious nodes in routing process for cluster based MANET have motivated us to propose an integrated solution for preventing malicious nodes in routing. Every member of cluster in a network monitors the behavior of each other in a cluster and updates their trust values. Our work proposes a well-defined trust election by considering various security parameters. The proposed work has the capability of preventing packet dropping packet injection, packet altering and packet misrouting attacks. Our work is compared with CBTRP and 2ACK. The simulation results illustrates that the proposed model can able to prolong the lifetime and forms stable clusters with most suitable one as cluster head and forwarder. This can be concluded that, our proposed approach would form the foundation for trust enabled and stable communication in MANET. The proposed work can be extended to design trustworthy forward paths to avoid link failures in a cluster based MANET routing.

REFRENCES:

[1] S. Basagni, M. Conti, S. Giordano, and I. Stojmenovic.Mobile ad hoc networking. Wiley, IEEE Press and John Wiley & Sons, New Jersey and New York, April 2004.

[2] A. Dana, A. M. Yadegari, M. Hajhosseini, T. Mirfakhraie, "A Robust Cross-Layer Design of Clustering-Based Routing Protocol for MANET," In Proceedings of International Conference on Advanced Communication Technology (ICACT), pages 1055-1059, February 2008.

[3] R. H. Hwang, C. Y. Wang, C. J. Wu and G. N. Chen, "A novel efficient power-saving MAC protocol for multi-hop MANETs," International Journal of Communication Systems, 26(1): 34-55, 2013.

[4] C. E. Perkins. Ad hoc networking.Addison-Wesley, 2001.

[5] E. M. Royer, C. K. Toh, "A review of current routing protocols for ad hoc mobile wireless networks," IEEE Personal Communications, 6(2): 46-55, 1999.

[6] Y. S. Chen, Y. C. Tseng, J. P. Sheu, P. H. Kuo, "An on-demand, linkstate, multi-path QoS routing in a wireless mobile ad-hoc network," Computer Communication, 27(1): 27-40, 2004.

[7] C. Perkins, E. Royer, S. Das, "Ad hoc on-demand distance vector (AODV)," In Proceedings of Second IEEE Workshop on Mobile Computing Systems and Applications, pages 90-100, February 1999.

[8] B. Liang, Z. J. Haas, "Hybrid routing in ad hoc networks with a dynamic virtual backbone," IEEE Transactions on Wireless Communications, 5(6): 1392-1405, 2006.

[9] P. Samar, M. R Pearlman, Z. J Haas, "Independent zone routing: An adaptive hybrid routing framework for ad hoc wireless networks," ACM Transactions on Networking, 12(4): 595-608, 2004.

[10] C.C. Tseng, K.C. Chen, "Organizing an optimal cluster-based ad hoc network architecture by the modified quine-mccluskey algorithm," IEEE Communication. Letter, 11(1): 43-45, 2007.

[11] M. Chatterjee, S. K. Das, D. Turgut, "WCA: A weighted clustering algorithm for mobile ad hoc networks," Cluster Computing Journal, 5(2): 193-204, 2002.

[12] A. Peiravi, H. R. Mashhadi and J. Hamed, "An optimal energy-efficient clustering method in wireless sensor networks using multi-objective genetic algorithm," International Journal of Communication Systems, 26(1): 114-126, 2012.

[13] R. Agarwal and M. Motwani, "Survey of clustering algorithms for MANET," International Journal on Computer Science and Engineering, 1: 98-104, 2009.

[14] M. Bechler, H.J. Hof, D. Kraft, F. Pahlke and L. Wolf, "A Cluster-based security architecture for ad hoc networks," In Proceedings of Twenty-third Annual Joint Conference of the IEEE Computer and Communications Societies, pages. 2393-2403, March 2004.

[15] C. Park, Y. H. Lee, H. Yoon, D. S. Choi and S. H. Jin. Cluster based trust evaluation in ad hoc networks. In Proceedings of International

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Conference on Advanced Communication Technology, pages 503-507, 21-23 February 2005.

[16] W.D Yang and G.Z Zhang. A weight- based clustering algorithm for mobile ad hoc network. In Proceedings of International Conference on Wireless and Mobile Communications (ICWMC '07), March 2007.

[17] Y. C. Hu, A. Perrig and D. B. Johnson. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks, 11(1-2): 21-38, 2005.

[18] X. Li, M. R. Lyu and J. Liu. A Trust Model Based Routing Protocol for Secure Ad Hoc Networks. In Proceedings of IEEE Aerospace Conference, pages 1286-1295, March 2004.

[19] S. Song, K. Hwang, R. Zhou, and Y.K Kwok. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Computing, 9(6): 24-34, 2005.

[20] A. Le, J. Loo, A. Lasebae, M. Aiash and Y. Luo. 6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach. International Journal of Communication System, 25(9): 1189-1212, 2012.

[21] Z. Liang and W. Shi. Analysis of ratings on trust inference in open environments. Perform Evaluation, 65(2): 99-128, 2008.

[22] P. Chatterjee. Trust Based Clustering And Secure Routing Scheme for Mobile Ad Hoc Networks. International Journal of Computer Networks and Communication, 1(2): 84-97, 2009.

[23] Q. Wang, J. Wang, J. Yu and Y. Zhang. Trust-aware query routing in P2P social networks. International Journal of Communication System, 25(10): 1260-1280, 2012.

[24] V. G. Rani and M. Punithavelli. Optimizing On Demand Weight-Based Clustering Using Trust Model for Mobile Ad Hoc Networks. International Journal of Ad Hoc and Ubiquitous Computing, 1(4): 81-91, 2010.

[25] C. Jianmin and W. Jie. A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks, 1-34, 2010.

[26] R. Ferdous, V. Muthukkumarasamy and E. Sithirasenan. Trust-Based Cluster Head Selection Algorithm for Mobile Ad Hoc Networks. In Proceedings of International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), pages 589 – 596, November 2011.

[27] B. Kadri, A. Mohamed and M. Feham. Secured Clustering Algorithm for Mobile Ad Hoc Networks. IJCSNS- International Journal of Computer Science and Network Security, 7(3): 27-34, 2007.

[28] BB. SathishBabu and P. Venkataram. A trust model for routing in MANETs: A cognitive agents based approach. In Proceedings of International Conference on Security and Management, pages 208-214, July 2011.

[29] H. Safa, H. Artail and D. Tabet. A cluster-based trust-aware routing protocol for mobile ad hoc networks. Wireless Networks, 16(4): 969-984, 2010.

[30] K. Liu, J. Deng, P. K. Varshney and K. Balakrishnan. An Acknowledgment-based Approach for the Detection of Routing Misbehavior in MANETs. IEEE Transactions on Mobile Computing, 6(5): 536-550, 2007.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

Table 2: *Weight Assignment To Trust Factors*

Value of trust parameter identification						**Weight assignment to trust factor**		
Trust parameters	**Node n_1**	**Node n_2**	**---**	**Node n_m**	**Average value (Avg)**	**Before sorting**	**After sorting (Descending order)**	**Weight assignment ($W_{d/m/f/a}$)**
pdr	$n_{1(d)}$	$n_{2(d)}$	**---**	$n_{m(d)}$	$pdr = \sum_{i=1}^{n} (\frac{d_i}{n})$	Pdr	pmr (W_m)	W_1
pmr	$n_{1(m)}$	$n_{2(m)}$	**---**	$n_{m(m)}$	$pmr = \sum_{i=1}^{n} (\frac{m_i}{n})$	Pmr	par (W_a)	W_2
pfr	$n_{1(f)}$	$n_{2(f)}$	**---**	$n_{m(f)}$	$pfr = \sum_{i=1}^{n} (\frac{f_i}{n})$	Pfr	pdr (W_d)	W_3
par	$n_{1(a)}$	$n_{2(d)}$	**---**	$n_{m(a)}$	$par = \sum_{i=1}^{n} (\frac{a_i}{n})$	Par	pfr (W_f)	W_4