Asian Journal of Information Technology 13 (9): 538-544, 2014
ISSN: 1682-3915

New Approach to Trust Evaluation for Cluster Based MANETS

[1]Rajkumar Mylsamy and [2]Subramanian Sankaranarayanan
[1]Department of Information Technology,
Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India
[2]Karpagam University, Coimbatore, Tamilnadu, India

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, researchers 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. The 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. Researchers compare the research with other clustering algorithms which are CBTRP and 2ACK. The analysis and simulation result clarifies that the proposed research effectually identifies and isolates malicious nodes and it outperforms the other algorithm.

Key words: Mobile ad hoc network, clustering, network security, privacy, routing protocols

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 (Basagni *et al*., 2004; Dana *et al*., 2008; Hwang *et al*., 2013; Perkins, 2001). Due to open working environment, MANETs are vulnerable to attacks by malicious nodes. Protocols used for routing in MANET can be classified as proactive (Royer and Toh, 1999), reactive (Chen *et al*., 2004; Perkins and Royer, 1999) or hybrid routing (Liang and Haas, 2006; Samar *et al*., 2004). 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 (Tseng and Chen, 2007; Chatterjee *et al*., 2002) 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 (Peiravi *et al*., 2013). A node that connects more than one adjacent cluster is called as gateway node (Agarwal and Motwani, 2009). Since, MANETs are infrastructure less and dynamic network, to protect this network from malicious nodes are hard to achieve. Existing trust value based protocols (Bechler *et al*., 2004; Park *et al*., 2005; Yang and Zhang, 2007) 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, researchers proposed their 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.

LITERATURE REVIEW

In this study, researchers present related works and background information for trust selection methods used in mobile ad hoc networks.

Corresponding Author: Rajkumar Mylsamy, Department of Information Technology,
Sri Krishna College of Engineering and Technology, Coimbatore, Tamilnadu, India

Several security routing algorithms (Hu *et al*., 2005; Li *et al*., 2004) 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 by Song *et al*. (2005) and Le *et al*. (2012) 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 (Liang and Shi, 2008; Chatterjee, 2009; Wang *et al*., 2012), 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 (Rani and Punithavelli, 2010; Chen and Wu, 2010). 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 research proposes a new algorithm, based on a De-Centralized algorithm. Many algorithms are proposed for trust identification of a node in cluster based routing for MANET. Trust value is evaluated by Ferdous *et al*. (2011) based on two parameters which is a self-evaluation of trust and sum of other nodes' trust evaluation. Trust value of a node is analyzed based on average trust value given by neighboring nodes in a cluster (Kadri *et al*., 2007). Trust is identified based on Behavior, Observation and Belief (BOB) of a node during protocol execution (Babu and Venkataram, 2011). In CBTRP (Safa *et al*., 2010), 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 by Liu *et al*. (2007). 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.

PROPOSED METHOD

The main objective of this study is to provide Security algorithms for cluster based MANET routing.

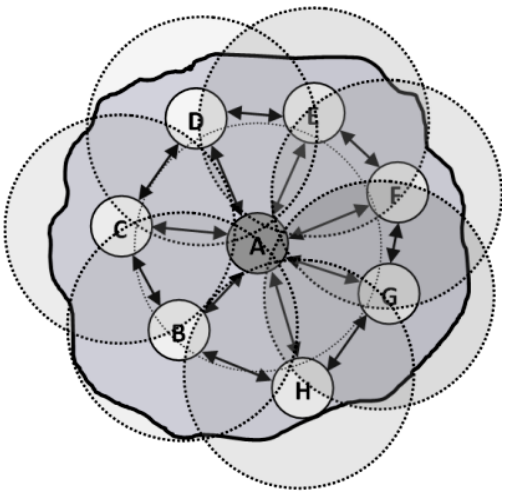

Fig. 1: Individual understanding of neighbor nodes

This proposed trust model comprises three modules, trust derivation, trust classification and trust computation. This model identifies malicious and non-malicious nodes in network.

Trust derivation: This module computes the trust value of a node in network. For example, 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. Figure 1 illustrates this.

Trust classification: Node's trust value is evaluated based on the following trust parameters:

- Packet Dropping Ratio (PDR)
- Packet Misrouting Ratio (PMR)
- Packet Falsely injected Ratio (PFR)
- 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).

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 $\{d_v<d_1,\ m_v>m_1,\ f_v<f_1,\ a_v<a_1\}$, $\{d_1\le d_v\le d_2,\ m_1\le m_v\le m_2,\ f_1\le f_v = f_2,\ a_1\le a_v\le a_2\}$ 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, respectively. Then, to determine range of values high, medium and low values 1, 0.5 and 0 are assigned. Trust classification is handled based on the Table 1.

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, researchers can protect same type of attack in the network. Weight assignment calculation is represented in Table 2. From this, researchers can identify the weighting coefficient value for individual trust parameters.

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 T_B^A 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.

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 neighbours. It evaluates the remaining number of nodes it can handle:

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

Where:

d_i = The degree of the node

S = The threshold value for all nodes in the respective cluster

The mobility of the node (Mob_{AB}): Mobility of the node at time t_2 is calculated using the Eq. 3:

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

where, p_1, q_1 and p_2, q_2 are the coordinates of the node at time t_1 and t_2, respectively. 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 neighbour table that is present in every member of cluster. Abstract data structure for construction of a cluster is called as Neighbour 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

Table 1: Trust classification

	Trust classification		
Trust identification	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	$a_v<a_1$	$a_1 \le a_v \le a_2$	$a_v>a_2$

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	Before sorting	After sorting (descending order)	Weight assignment ($W_{d/m/f/a}$)
PDR	n_1(d)	n_2(d)	---	n_m(d)	$PDR = \sum_{i=1}^{n}(d_i/n)$	PDR	PMR (W_m)	W_1
PMR	n_1(m)	n_2(m)	---	n_m(m)	$PMR = \sum_{i=1}^{n}(m_i/n)$	PMR	PAR (W_a)	W_2
PFR	n_1(f)	n_2(f)	---	n_m(f)	$PFR = \sum_{i=1}^{n}(f_i/n)$	PFR	PDR (W_d)	W_3
PAR	n_1(a)	n_2(d)	---	n_m(a)	$PAR = \sum_{i=1}^{n}(a_i/n)$	PAR	PFR (W_f)	W_4

node identification (MAC ID) IDs to reach adjacent cluster heads. Communication of CH with an adjacent cluster is handled by gateway node.

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 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.

Route discovery and route recovery: This study describes the 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 1 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 <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.

SIMULATION RESULTS

Simulation parameters: The proposed research 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 m. The radio model is simulated with a nominal bit rate of 11 Mbp. The traffic type is Constant Bit Rate (CBR) with network packet rate of 4 packets sec^{-1} and the packet size is 512 bytes. The movement model used is a Random way point model. The pause time used is 0 sec. The simulation time used is 800 sec. The value of high, medium and low for trust classification are 1, 0.5 and 0, respectively. The value of weights W_1, W_2, W_3 and W_4 for simulations are 0.1, 0.2, 0.3 and 0.4, respectively. The value of weights for identifying stability factors S_1 and S_2 are 0.5 and 0.5, respectively. The value of d factors for packet delivery ratio d_1 and d_2 are 5 and 10%.

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 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.

Control overhead: The ratio of the number of control packets (route request, route reply, error packets,

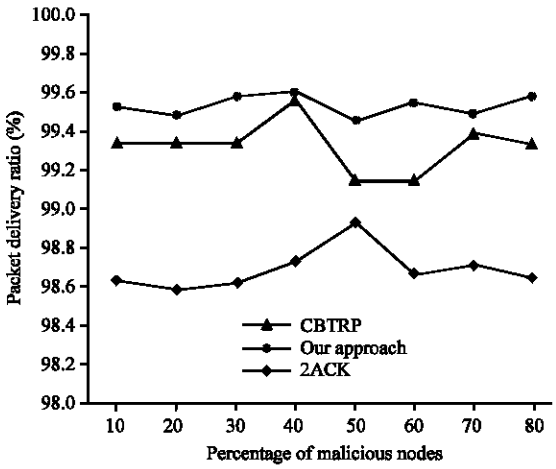

Fig. 2: Packet delivery ratio of our approach, CBTRP and 2ACK

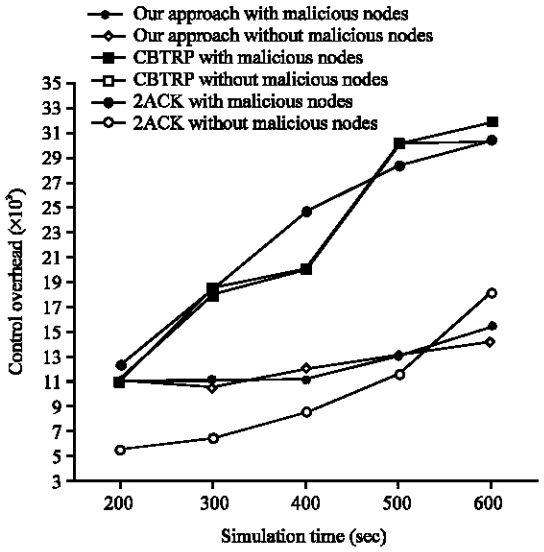

Fig. 3: Control overhead of our approach, CBTRP and 2ACK

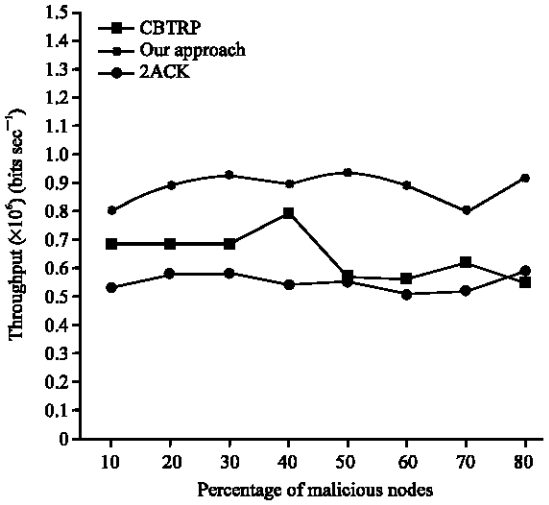

Fig. 4: Throughput average of our approach, CBTRP and 2ACK

sequencing) transmitted to the number of data packets delivered is defined as control overhead. Figure 3 shows that our approach is very efficient in terms of control overhead in data delivery. The research analyses the control overhead in our approach, CBTRP and 2ACK on two conditions (with and without considering malicious nodes). Control overhead of our approach is less than CBTRP and 2ACK. The proposed approach does not do cluster head re-election process periodically for cluster maintenance.

Throughput: The percentage of misbehaving nodes versus average aggregated throughput is shown in Fig. 4.

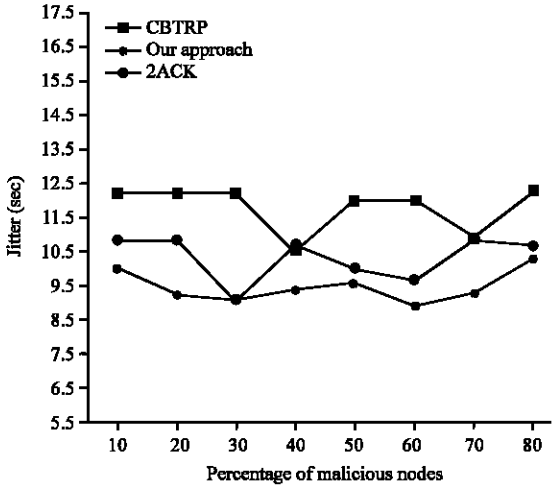

Fig. 5: Packet latency (Jitter) of our approach, CBTRP and 2ACK

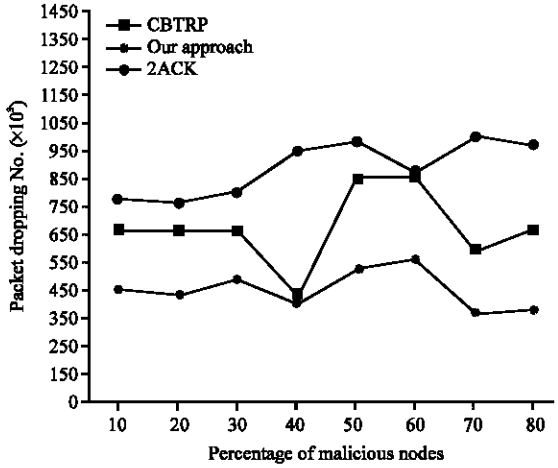

Fig. 6: Packet drop level of our approach, CBTRP and 2ACK

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 20-80% of total nodes and the results show that the proposed method outperforms CBTRP and LEACH in terms of throughput.

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. Jitter also called as packet delay variation can result in both increased latency and packet loss. As Fig. 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 research considers individual trust

parameters for isolating misbehaving nodes, it protects same node is affected. It is significantly less compared to others.

Packet dropping: Figure 6 shows the result of packets drop for the schemes when the number of misbehavior node is increased. From the result, researchers can see that the proposed research 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.

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. Research proposes a well-defined trust election by considering various security parameters. The proposed resaerch has the capability of preventing packet dropping packet injection, packet altering and packet misrouting attacks. Research 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 the proposed approach would form the foundation for trust enabled and stable communication in MANET. The proposed research can be extended to design trustworthy forward paths to avoid link failures in a cluster based MANET routing.

REFERENCES

Agarwal, R. and M. Motwani, 2009. Survey of clustering algorithms for MANET. Int. J. Comput. Sci. Eng., 1: 98-104.

Babu, B.S. and P. Venkataram, 2011. A trust model for routing in MANETs: A cognitive agents based approach. Proceedings of the International Conference on Security and Management, July 18-21, 2011, Las Vegas, VA., USA., pp: 208-214.

Basagni, S., M. Conti, S. Giordano and I. Stojmenovic, 2004. Mobile Ad Hoc Networking. John Wiley and Sons Inc., New York, USA.

Bechler, M., H.J. Hof, D. Kraft, F. Pahlke and L. Wolf, 2004. A cluster-based security architecture for ad hoc networks. Proceedings of the 23rd IEEE Computer and Communications Societies Annual Joint Conference, March 7-11, 2004, Hong Kong, China, pp: 2393-2403.

Chatterjee, M., S.K. Das and D. Turgut, 2002. WCA: A weighted clustering algorithm for mobile Ad Hoc networks. Cluster Comput., 5: 193-204.

Chatterjee, P., 2009. Trust based clustering and secure routing scheme for mobile Ad Hoc networks. Int. J. Comput. Networks Commun., 1: 84-97.

Chen, J. and J. Wu, 2010. A survey on cryptography applied to secure mobile ad hoc networks and wireless sensor networks. pp: 1-34. http://www.cse.fau.edu/~jie/research/publications/Publication_files/wsn-chapter.pdf.

Chen, Y.S., Y.C. Tseng, J.P. Sheu and P.H. Kuo, 2004. An on-demand, link-state, multi-path QoS routing in a wireless mobile ad-hoc network. Comput. Commun., 27: 27-40.

Dana, A., A.M. Yadegari, M. Hajhosseini and T. Mirfakhraie, 2008. A robust cross-layer design of clustering-based routing protocol for MANET. Proceedings of the 10th International Conference on Advanced Communication Technology, Volume 2, February 17-20, 2008, Gangwon-Do, Korea, pp: 1055-1059.

Ferdous, R., V. Muthukkumarasamy and E. Sithirasenan, 2011. Trust-based cluster head selection algorithm for mobile ad hoc networks. Proceedings of the IEEE 10th International Conference on Trust, Security and Privacy in Computing and Communications, November 16-18, 2011, Changsha, China, pp: 589-596.

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

Hwang, R.H., C.Y. Wang, C.J. Wu and G.N. Chen, 2013. A novel efficient power-saving MAC protocol for multi-hop MANETs. Int. J. Commun. Syst., 26: 34-55.

Kadri, B., A. M'hamed and M. Feham, 2007. Secured clustering algorithm for mobile ad hoc networks. Int. J. Comput. Sci. Network Secur., 7: 27-34.

Le, A., J. Loo, A. Lasebae, M. Aiash and Y. Luo, 2012. 6LoWPAN: A study on QoS security threats and countermeasures using intrusion detection system approach. Int. J. Commun. Syst., 25: 1189-1212.

Li, X., M.R. Lyu and J. Liu, 2004. A trust model based routing protocol for secure ad hoc networks. Proceedings of the IEEE Conference on Aerospace, Volume 2, March 6-13, 2004, Big Sky, Montana, USA., pp: 1286-1295.

Liang, B. and Z.J. Haas, 2006. Hybrid routing in ad hoc networks with a dynamic virtual backbone. IEEE Trans. Wireless Commun., 5: 1392-1405.

Liang, Z. and W. Shi, 2008. Analysis of ratings on trust inference in open environments. Perform. Eval., 65: 99-128.

Liu, K., J. Deng, P.K. Varshney and K. Balakrishnan, 2007. An acknowledgment-based approach for the detection of routing misbehavior in MANETs. IEEE Trans. Mobile Comput., 6: 536-550.

Park, C.I., Y.H. Lee, H. Yoon, D.S. Choi and S.H. Jin, 2005. Cluster-based trust evaluation in ad hoc networks. Proceedings of the 7th International Conference on Advanced Communication Technology, February 21-23, 2005, Dublin, Ireland, pp: 503-507.

Peiravi, A., H.R. Mashhadi and S.H. Javadi, 2013. An optimal energy-efficient clustering method in wireless sensor networks using multi-objective genetic algorithm. Int. J. Commun. Syst., 26: 114-126.

Perkins, C. and E. Royer, 1999. Ad hoc on-demand distance vector routing. Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, February 25-26, 1999, New Orleans, LA., USA., pp: 90-100.

Perkins, C.E., 2001. Ad Hoc Networking. Addison-Wesly, Boston, MA., USA.

Rani, V.G. and M. Punithavelli, 2010. Optimizing on demand weight-based clustering using trust model for mobile ad hoc networks. Int. J. Ad Hoc Sensor Ubiquitous Comput., 1: 81-91.

Royer, E.M. and C.K. Toh, 1999. A review of current routing protocols for ad hoc mobile wireless networks. IEEE Persnol Commun., 6: 46-55.

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

Samar, P., M.R. Pearlman and Z.J. Haas, 2004. Independent zone routing: An adaptive hybrid routing framework for ad hoc wireless networks. IEEE/ACM Trans. Networking, 12: 595-608.

Song, S., K. Hwang, R. Zhou and Y.K. Kwok, 2005. Trusted P2P transactions with fuzzy reputation aggregation. IEEE Internet Comput., 9: 24-34.

Tseng, C.C. and K.C. Chen, 2007. Organizing an optimal cluster-based ad hoc network architecture by the modified Quine-McCluskey algorithm. IEEE Commun. Lett., 11: 43-45.

Wang, Q., J. Wang, J. Yu, M. Yu and Y. Zhang, 2012. Trust-aware query routing in P2P social networks. Int. J. Commun. Syst., 25: 1260-1280.

Yang, W.D. and G.Z. Zhang, 2007. A weight-based clustering algorithm for mobile ad hoc network. Proceedings of the 3rd International Conference on Wireless and Mobile Communications, March 4-9, 2007, Guadeloupe, pp: 3-3.