Asian Journal of Information Technology 15 (19): 3756-3762, 2016
ISSN: 1682-3915


# Optimizing Trust Based Secure Routing for Unified Efficient Resource Sharing for Large Scale MANET-TSRRS

[1]R. Dhanapal and [2]P. Visalakshi
[1]Department of ECE, Anna University, Chennai, Tamil Nadu, India
[2]Department of ECE, PSG College of Technology, Coimbatore, Tamil Nadu, India

**Abstract:** In this research study, a cross layer framework is proposed for secure clustering scheme in mobile adhoc networks which includes the network initialization stage, clustering scheme, security phase and routing policy.The framework employs distributed clustering scheme which is referred to as HAABO. The objective is to achieve good scalability, security, energy consumption and long network life time in large scale network. The network initialization stage is selective solution used to reduce the link loss and measure the signal strength of the link using RSSI value. The clustering scheme is a load balancing solution for homogenous and heterogeneous cluster formation using HAABO. The security scheme is a preventive solution that enables secure trust based public authentication service based on the trust model communication using improved unified trust management scheme. A key-encrypted onion is used to record the route discovered and validating the packet request per hop by using group signature. The routing policy is a corrective solution to predict the geographical location node mobility and reduces routing redundancy.

**Key words:** Hybrid routing, trust management, clustering scheme, HAABO, routing policy, security

## INTRODUCTION

A network which contain mobile or fixed wireless devices communication among without any centralized infrastructure is known as Mobile Ad hoc Network (MANET). MANETS does not depend upon additional hardware, to show them as an ideal candidate for recovery and emergency operations. They possess a limited transmission range for each node to seek its neighboring node's assistance in forwarding packets. Configured routing protocols are employed to create routes among the nodes which are farther than a single hop.

The exclusive feature of the protocols is tracing the routes in spite of a dynamic topology. There are two phases of communication in mobile ad hoc networks, neighbor discovery and data transmission. In a conflicting environment, both phases are accessible to a variety of attacks. The attackers can hinder the propagation of certain controllingroutes the traffic and unfortunately the topological knowledge of benign nodes is being dominated.

For a complete security in both phases of a MANET, secure routing protocols are essential because nodes complicated in the routing process cannot assure security and undisrupted data transmission. Therefore, misbe having nodes could accept with the route discovery and they can be placed on the available routes. The events that cannot match with the malevolent disruptions of data transmission are upper layer mechanisms like mechanisms considered by the MANET routing protocols or reliable transport protocols. The communicating nodes can mislead for long time period, imagining that there is proper flow of data when there is loss of communication. A new security problem arises in ad hoc network operations. They are easily accessed to physical security threats.

Fixed network security approaches are unachievable because of the noticeable characteristic of the ad hoc networks. Raising new internal malicious node's threads are difficult to defend. To adapt special characteristics of ad hoc network new security mechanisms are adapted. A new method is proposed to ensure security in both the phases. For ensuring routing phase security, trust based path routing protocol is processed. It follows a secured path with minimal overhead. The trust value of the nodes prohibits misbehaving nodes.

Security solutions associated with static configuration can't be ample because of the dynamic topology of the networks. Furthermore, the power accountable for key distribution of the whole network is

**Corresponding Author:** R. Dhanapal, Department of ECE, Anna University, Chennai, Tamil Nadu, India

liable to single point failure. To overcome this, a distributed architecture needs for better functionality. All the nodes should be adapted to operate in a mode that it should not trust on any peer quickly.

Since, the trust relationship is available for the entire node, it becomes simple to choose proper security measures for providing required protection. Finally, hostile service requests can be rejected or ignored. The entire network in ad hoc network is coordinated by default and these trust relationships are extremely responsive to attacks. The major challenges related to securing ad hoc networks are:

- To prepare the ad hoc network work thoroughly secured against different external and internal attacks
- The security solutions should contain sufficient energy
- To achieve the functionality of the network (routing the packets properly and securely) when some of nodes are being captured or any node goes beyond the radio range due to node mobility

The nodes are grouped into clusters for avoiding the overhead in handling the network. A trust based approach for distributed cluster formation is discussed in which ad hoc network is viewed as a set of self-organizing clusters. It is based on the trust relationship between the neighbor nodes. Each cluster is a group of nodes headed by a single node, Cluster Head (CH). Cluster head is selected by member nodes to design the more stable cluster head upon some metrics. It is a distributed and secured selection.

By formalizing trust relationship, the challenges can be faced among the nodes. Some methods are employed for quantifying the trust depending upon some metrics. From the requirement, these nodes can be chosen. To maintain the trust of a particular node, nodes monitor tracks the information from the other nodes and takes decisions about the node. To obtain the resultant trust, the direct trust values are considered and recommended from other nodes and mathematical model of Dempster-shafer of combining evidences are used and it calculates the most probable trust value of a particular node.

A quantitative trust evaluation algorithm is maintained at each node to evaluate the direct trust of its neighbor nodes. All the nodes undergo periodic monitoring by other nodes to enquire is there any malicious or selfish activity.

**Literature review:** To have a secure data transmission, trustworthy area of mobile and ad hoc network is needed. The most used approaches are based on public-key certificates. It has paved the way for miscellaneous trust models ranging from centralized models to web-of-trust and distributed certification authorities. Nodes mobility freedom has constraints while designing reliable certification systems. These issues are addressed and a secure and reliable certificate chains are discussed for the recovery process of every protocol in the mobile ad hoc networks. It is based on web-of-trust so that the users assure the role of certificates by themselves while issuing and managing public-key certificates (Omar *et al*., 2016).

Establishing network among nodes requires trust management in MANETs with appropriate trust levels. It offers network security services like access management, malicious node detection, secure resource sharing and authentication. The trust management is a multifunctional control method possessing a trust between the neighbouring nodes and to make a routing path. It projects new data-monitoring theme for trust management on MANETs using autonomic principles. It imposes secured routing path selection based on trust values of nodes (Supriya *et al*., 2015).

In MANET's, the participating nodes authorize a network with the help of Trust management with fewer interactions and with acceptable trust level. Trust system are employed for administering network security services like access control, malicious node detection, secure resource sharing and authentication. So that node's trust values are calculated periodically on trust metrics and computational methods. A trust based packet forwarding scheme for detecting and isolating the malicious nodes are designed which uses routing layer information (Charumathi and Chatterjee, 2014).

In direct observation, from an observer node trust value is calculated to observed node and the indirect observation also known as second hand information is accessed from neighbour nodes of the observer node and the trust value is calculated. It improves throughput and packet delivery ratio in the network. A new group mobility model is discussed in which the number of groups are moved along the stimulated area and the individual static node in the connected area reports one group activity to other group. Nodes in the same group have same average velocity in the area of simulation (Jain *et al.,* 2013). To secure data in data transmission, cryptographic mechanism are used to acquire high computational cost and inability to identify the nodes with malicious

intention. Therefore employing cryptographic techniques in MANET becomes impossible. So that Trust mechanism is used instead of cryptographic technique. Trust mechanism protects data forwarding by isolating nodes with malicious intention using trust value on the nodes.

Trust Based Secure Routing Protocol (TBSRP) is designed for security. It is a hybrid approach, a reliable node is identified and communication is preferred in that node. It is an effective and reliable communication approach which has ability to decide selection on next hop under the trust vector and the data can be transmitted only via the trustful node.

An overview of reputation-based approaches is provided to improve the trusted functionality in ad hoc distributed resource-sharing networks. The investigations are done on the basis of several reputation and trust metrics for protection. The general and function specific issues are studied and the requirements for those functions are estimated (Hatzivasilis and Manifavas, 2012). The Trust based routing protocol is discussed which uses fuzzy logic rules prediction method. Untrustworthiness is removed in the nodes for obtaining a reliable path along the source and destination. It is a new Multipath proactive routing protocol on the basis of the multipath OLSR (Geatha and Ramani, 2012).

The different mobility models and their advantage and disadvantages are studied and they are being considered in overcoming the future model (Vasanthi *et al*., 2011). The transactions become less secure because of the fixed infrastructure less environment. The cryptographic techniques for a secure transmission are not accepted by the traditional routing algorithms in MANETs. A secure, trusted, optimal scheme for routing in MANETs is discussed (Neelakandan and Anand, 2011).

The total energy consumed in the data transfer path is minimized to increase the network life time. The clusters create hierarchical WSNs to provide incorporate efficient utilization of limited resources of sensor nodes. A taxonomy of energy efficient clustering algorithms, timeline and description of LEACH in WSNs, are discussed (Kumar *et al*., 2011).

Mobile Ad-hoc Networks (MANETs) have issues in resources sharing since they are associated via mobile nodes without any prior knowledge of the existing nodes. The main scope is to formalize a trust mechanism for MANETs. The node metrics are provided to manage trust and to take decision on grouping and or pairing keys in the network. The routing protocols of ad-hoc networks are analysed with consideration for trust and Dynamic Source Routing (DSR) protocols are selected and used in distributed ad hoc network settings for path discovery (Ferdous *et al*., 2010).

A distributed self-organizing trust based clustering framework is discussed to provide security to ad-hoc networks. The trust evaluation algorithm is employed at each node to determine the direct trust rating normalized as a fuzzy value between zero and one. The evidence theory of Dempster-Shafer considered for combining the evidences collected by a cluster head itself and the recommendations from other neighbour nodes.

A critical issue in a practical network is the transmitting message securely. In a multi-hop network, it is even more critical and so it is better to ensure trust level in the forwarding nodes. But the value of trust changes with time, give rise to malicious node and vice versa. The message contents should not be delivered to the intermediate nodes and protection is needed for that. Increased computation is necessary for encrypting and also for integrity of messages. An approach work is introduced to overcome the problems and having minimum number of overheads (Dhurandher and Mehra, 2009).

## MATERIALS AND METHODS

**Proposed work:** In this study, the explanation of proposed Trust based Secure Routing for unified Resource Sharing (TSRRS) and its implementation is presented. The management of trust scheme for secure access and the clustering scheme using HAABO is implemented for load balancing and trust communication. Both models combine to have an efficient sharing of resources with secure routing in large scale MANET.

**Network initialization stage:** The stage of initialization is considered during the deployment of the MANET. It determines the each stage of network length according to the deployment characteristics and network needs. The stage of data push, synchronization and data pull will be in active mode and the idle stage is in inactive mode. Each active stage function is related to the servers and the tasks are related to the clients.

The initialization of the network is considered with the various numbers of parameters involvements and each network node is initialized with the same values of parameters. The parameter values are static during the deployment of the MANET. The management of the database is expected to be fully replicated by the server. As well as, the locations are monitored independently by the each client and server in the cycle of service as per the common parameters and it is used for synchronization with other nodes.

## RESULTS AND DISCUSSION

**Clustering scheme based on HAABO:** In order to have efficient data validation and network lifetime the cross layer design is developed with the efficient distribution of cluster head. The selection process is carried out by proposing the Hybrid AABO based on the state variables like range of transmission, initial energy, Receiver Signal Strength Indicator (RSSI), the node and sink distance, optimal number of clusters, mobility and the differences of degree. The Hybrid AABO protocol is an effective processing of message exchange and complexity.

In Hybrid AABO, the cluster head selection and the formation is carried out in cluster setup phase. By state variables the cluster is formed and it is maintained by the agents (onlooker ant,employed bee and scout bees). The data receiving from the cluster nodes to the cluster head is processed in the phase of steady state. It performs the data transfer at fixed interval to the sink and the aggregation of data. The initial energy of the node is estimated as given as:

$$E_I = E_{Tx} + E_{Rx} \tag{1}$$

The range of the transmission in the network will be same for the entire node. By using exponential weighted moving average the node mobility is estimated and by using a geometric progression method the distance between the sink and the node is calculated and represented by the common ratio and the first term. The distance is based on the intermediate node of the location services. The series and the selection of cluster head are estimated as given as:

$$T = 1-\alpha\times(t''+\alpha\times t') \tag{2}$$

$$\Sigma_{k=0}^{n-j}(\alpha r^K)=\alpha\left(\frac{1-r^n}{1-r}\right) \tag{3}$$

$$F(CH) = \left( \begin{matrix} w_1 \\ RSSI \end{matrix} \times EI \times \begin{matrix} w_2 \times d + w_3 \\ + W_4 + ND + W_5 \end{matrix} dis \right) \tag{4}$$

As per the procedure the selection and the formation of cluster is carried out.

**Algorithm:** Cluster scheme using HAABO protocol
**Input:** SN solutions, colony size
**Output:** Optimized solution for cluster formation
For i = 1 to SN
Calculate the values of fitness for the selection of cluster head using Eq. 4
End the loop
Send the employed bees out
For i = 1 to SN
Estimate the neighbour solution

$$v_{ij} = x_{ij}\,\phi_{ij}\,(x_{ij} - x_{kj}) \tag{5}$$

7.For j = 1 number of nodes
8.Join the regular nodes in to cluster head nearest based on the node distance, RSSI and cluster head.
9.End the loop
10.Estimate the values of fitness using (Ambatkar and Selokar, 2014)
11.The pheromone trail calculation

$$t(i) = \left\{ \begin{matrix} t\geq 0 \text{ for} \dfrac{f(CH)}{1+f_i} \\ t<0\, 1+\alpha bs(f_i) \end{matrix} \right\} \tag{6}$$

12.Apply the process of greedy selection
13.End the loop
14.Probability values estimation:

$$P(i) = \frac{(0.09)\times t(i)}{\Sigma_{i\leq j\leq mt(j)}^{SN}} \tag{7}$$

15.Send onlooker bee out
16.For i = 1 to SN
17.Choose the solutions based on the probabilities
18.Repeat the process from 6-12
19.End the loop
20.Memorize the best solution
21.Send the scout bees
22.Until the condition satisfied replace the
ababdoned solution with the new produced

**Improved unified trust management scheme:** In a MANET, trust is referred as a degree in a network. It is characterized into context dependency, non-transitivity, subjectivity, asymmetry and dynamicity. Context dependency is the assessment of trust based on the node etiquette and various actions facet is evaluated by the trust.Non-transitivity referred as, if node A trust on B and B on C then there is not essential A to trust C. The observed node decision is if done with the right of the observer node is referred as subjectivity. Asymmetry means, if node A trusts on B then there is not necessary for B to trust on A. As per the node etiquette, the trusted node changes by depending on it is referred as dynamicity. The calculation of trust with indirect and direct observation is considered as follow.

**Direct:**

- Let Node A is an observer node and its one-hop neighbor Node B is a trustee node to receive the packet
- Number of packets received is incremented by 1
- If Node A acknowledges that Node B sends packet successfully

- Then, the number of packets forwarded is incremented by 1
- Else if the TTL of the packet becomes null or buffer overflows at Node B or the wireless connection state at Node B is poor then
- The number of packets received is depreciate by one
- Trust value is calculated and updated

Indirect:

- If Node A, an observer discovers more than one hop neighbors between it and the trustee that is Node B then
- Calculation on trust value is performed
- Else the trust value is designated as zero

**Secure routing process based on trust:** The secure process of routing is processed by the associate approach rule based on the trust. The route of the node from source to destination is carried out by sending messages to the neighboring node. It will continue till it reaches the destination node and it passes it by the predefined threshold based on trust analysis. The transmitting of packet is processed by route selection and applying the waiting interval till the confirmation of packet received from the destination.

After receiving the reply message is carried out similarly and also not essential to use constant route. As well as the reply message is verified whether it is valid to continue with the selected path and it is updated the route. If no reply from destination with the time slot preferred then the source can process the trust analysis on routing by statistics reduction of trust worth.

Also, the response node in underlying route is said to be positive by the source node if it is malicious and it places the blacklist by setting the value to zero. The best route is selected for transmission if the selected rout is not valid then it moves to next route to process. It is enforced the proposed protocol based on the HAABO routing and the mechanism of trust analysis.

```
For n = 1 to i
Request to Node (i) for communication using P-key
If
(Accepted (response) = valid)
Set trust (node (i) = 1}
Else
Set trust (node (i) = 0)
Define compromising node and set c-node  = source
If
Trust (node (i) = 1)
If (Res-Time (node (i)<I-threshold) and throughput (node (i)) >H-Threshold)
and energy (node (i)>E-Threshold))
Set T-Node(i) = 1 and as eligible node for next node communication
Set C-Node = Node (i)
Else
Set T-Node (i) = 0; Print "Not Trustworthy"
Determine most Eligible node from the list of neighbour in terms of response
time and replace node (i) with the node.
Node (i) = Eligible neighb our node and  set  c-node source
End for loop
```

In this study the simulation result is carried out by implementing using NS2 tool and consists with the analysis of performance and comparison between various existing approaches and the proposed approach (Table 1).

The analysis of performance is illustrated between the numbers of nodes Vs average end to end delay, packet delivery ratio, routing overhead and energy usage are shown in Fig 1-4 respectively. Also, the performance analysis of malicious node Vs packet delivery ratio, average data delivery latency and control message are shown in Fig 5-7 respectively.

Table 1: Simulation parameter for the network establishment

| Parameters | Value |
|---|---|
| Simulator | NS-2 (v2.34) |
| Topology size | 1200×1200 m |
| Number of nodes | 200,400,600,800,1000 |
| Transmission range | 200 m |
| Bandwidth | 2Mbps |
| Interface queue length | 100 |
| Traffic type | CBR |
| MAC type | 802.11 |
| Packet size | 512 bytes |
| Paused time | 0s |
| Speed | 5 (m $sec^{-1}$) |

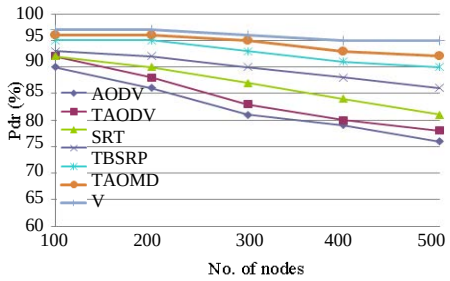


Fig. 1: No of nodes vs packet delivery ratio

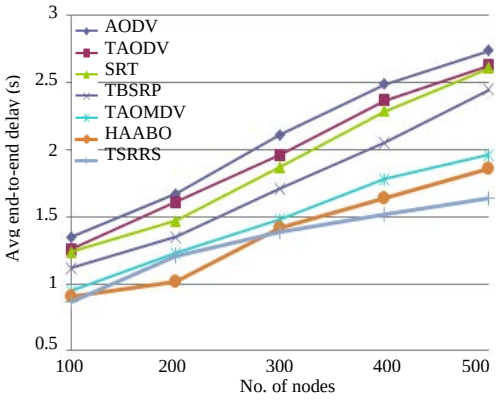


Fig. 2: No. of nodes vs average end-to-end delay

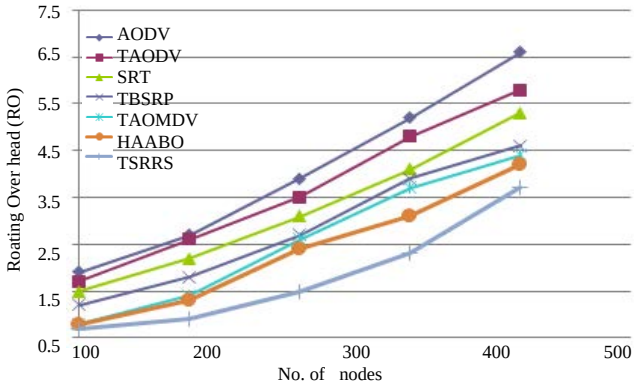


Fig. 3: No of nodes vs routing overhead

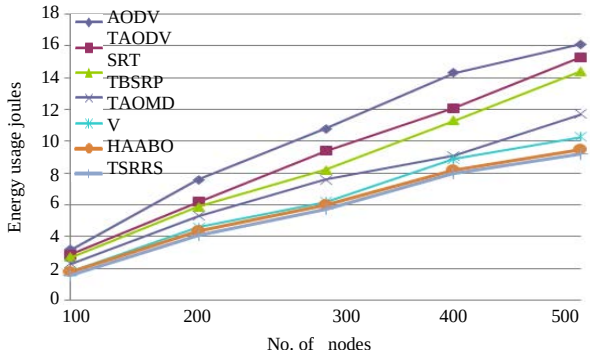


Fig. 4: No of nodes vs energy usage

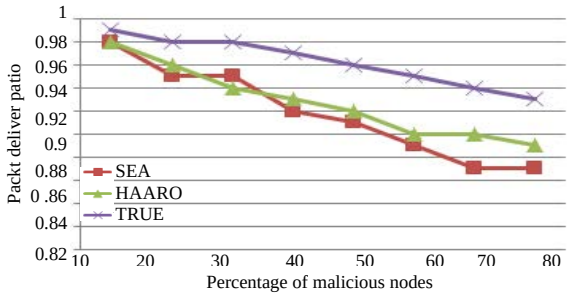


Fig. 5: Percentage of malicious node vs packet delivery ratio

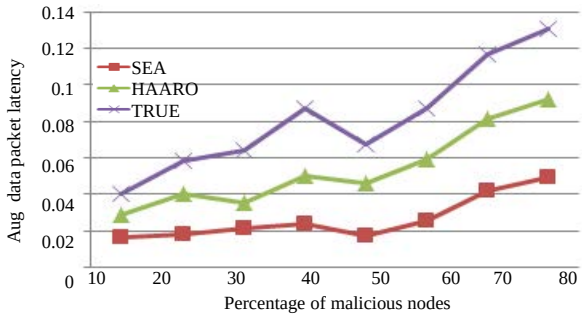


Fig. 6: Percentage of malicious node vs average data packet latency

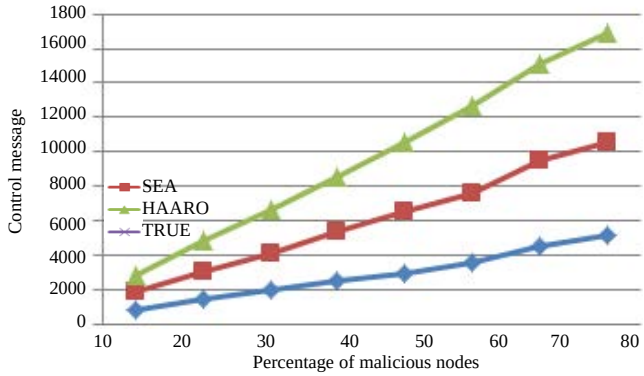


Fig. 7: Percentage of malicious node vs control message

## CONCLUSION

In this study, the proposed approach provides a lower packets loss ratio and higher throughput in various outlines of mobile in the occurrence of adversary attacks. Also, it delivers improved maintenance for the safe communications that are delicate to packet loss ratio and reduced the delay of packet. The routing is carried out based on trust with the combination of protocol and trust based management scheme. The detecting of failure link is considered more active and initiated either by the challenger attacks or mobility. In MANET's the trust value of nodes observed in unreliable reasoning using current improvements.

## REFERENCES

Ambatkar, R. and P. Selokar, 2014. A literature review of enhancing security in mobile ad-hoc networks using trust management security scheme. Int. J. Sci. Res. (IJSR), 3: 1380-1382.

Charumathi, K.S. and M. Chatterjee, 2014. Knowledge based trust for secure routing process in mobile ad-hoc networks. Int. J. Res. Stud. Comput. Sci. Eng. (IJRSCSE), 1: 63-74.

Dhurandher, S.K. and V. Mehra, 2009. Multi-path and message trust-based secure routing in ad hoc networks. Proceedings of the ACT'09 International Conference on Advances in Computing Control and Telecommunication Technologies, December 28-29, 2009, IEEE, New Delhi, India, ISBN: 978-1-4244-5321-4, pp: 189-194.

Ferdous, R., V. Muthukkumarasamy and A. Sattar, 2010. Trust formalization in mobile ad-hoc networks. Proceedings of the 2010 IEEE 24th International Conference on Workshops Advanced Information Networking and Applications (WAINA), April 20-23, 2010, IEEE, Perth, Western Australia, ISBN: 978-1-4244-6701-3, pp: 351-356.

Geetha, S. and G.G. Ramani, 2012. Trust based secure multipath OLSR routing protocol in MANET using fuzzy theory. Proceedings of the 2nd International Conference on Computational Science Engineering and Information Technology, October 26-28, 2012, ACM, Coimbatore, India, ISBN: 978-1-4503-1310-0, pp: 120-125.

Hatzivasilis, G. and C. Manifavas, 2012. Building trust in ad hoc distributed resource-sharing networks using reputation-based systems. Proceedings of the 2012 16th Panhellenic Conference on Informatics (PCI), October 5-7, 2012, IEEE, Piraeus, Greece, ISBN: 978-1-4673-2720-6, pp: 416-421.

Jain, D., A. Payal and U. Singh, 2013. Sensor nodes based group mobility model (SN-GM) for MANET. Int. J. Sci. Eng. Res., 4: 823-830.

Kumar, V., S. Jain and S. Tiwari, 2011. Energy efficient clustering algorithms in wireless sensor networks: A survey. Int. J. Comput. Sci. Issues, 8: 259-268.

Neelakandan, S. and J.G. Anand, 2011. Trust based optimal routing in MANET's. Proceedings of the 2011 International Conference on Emerging Trends in Electrical and Computer Technology (ICETECT), March 23-24, 2011, IEEE, Tamil Nadu, Indian, ISBN: 978-1-4244-7923-8, pp: 1150-1156.

Omar, M., H. Boufaghes, L. Mammeri, A. Taalba and A. Tari, 2016. Secure and reliable certificate chains recovery protocol for mobile ad hoc networks. J. Network Comput. Appl., 62: 153-162.

Supriya, L.S., V.M. Purohit and R.G. Ranjana, 2015. A trust model for self organized mobile ad-hoc network. Int. J. Emerging Technol. Adv. Eng., 5: 58-64.

Vasanthi, V., M. Romenkumar, N. Ajithsingh and M. Hemalatha, 2011. A detailed study of mobility models in wireless sensor networks. J. Theor. Appl. Inf. Technol., 33: 7-14.