Middle-East Journal of Scientific Research 25 (1): 95-101, 2017
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2017.95.101

An Integrated Trust based Inter-Cluster and Intra-Cluster Communication for Secure Multicast Routing in MANETs

[1]C. Vijayakumaran, [2]T. Adiline Macriga and [1]S. Veenadhari

[1]Computer Science and Engineering, AISECT University, Bhopal, India
[2]Sri Sairam Engineering College, India

Abstract: Trust based clustering approaches have been the research interest amongst researchers in the area of Mobile Adhoc Networks (MANETs) since their inception. It is essential to ensure the security of nodes in such network environment, since nodes are susceptible to different kinds of security threats. In order to achieve scalabili head node. Intra cluster and inter cluster nodes communication are achieved through multi-hop communication between nodes without affecting network services. In this paper, the trustworthiness of nodes is evaluated by involving neighbor nodes with a Cooperative Trust Establishment approach without having any fixed central authorities. An integrated trust based multicast routing approach is proposed to construct secure forwarding path between a sender and a receiver node in the inter and intra cluster communication environment. The most stable trusted node is selected as a Certificate Authority (CA) which provides authentication and integrity of a trustable node in order to defend the network resources from potential attackers. The proposed approach shows a significant improvement in the detection ty, hierarchical clustering approach is used in network topology construction process. Every clusters have mobile nodes and a of malicious nodes within a cluster, provides better packet delivery ratio and reduce communication overheads occurred due to security threats.

Key words: Trust based Clustering approach · Mobile Adhoc Networks (MANETs) · Hierarchical Clustering · Intra Cluster and Inter Cluster Communication · Cooperative Trust Establishment and Certificate Authority(CA)

INTRODUCTION

A mobile adhoc network (MANET) is a kind of wireless network that consists of self-configurable, low energy mobile nodes without having any fixed infrastructures as available in the case of wireless LANs and cellular networks. The nodes in the adhoc network create frequent network partitions due to mobility results in dynamic network topologies. The dynamic topological nature of the adhoc network paves a way to insecure communication between nodes and also needs multi-hop communication between nodes to forward a packet between them. Frequent link failure causes high error rate and communication channel become vulnerable to various security attacks. In wired network scenario, link failures are very rare event since network condition is always static. Moreover, error rate is also quite low compared to wireless network.

Multicast routing [1] enables group members to receive the messages sent by a sender. Establishment of secure route in adhoc network is an expensive process. In order to simplify the routing process, it is useful to collate the routes to a sub-structure of the network. It provides a convenient way to send and receive local data packets on a short path within the group members of the sub-structure. These sub-structures of network can be termed as clusters and the communication between the group members within a cluster is known as intra cluster communication. It is also possible to setup long routing paths that provides efficient communication between different sub-structures of the network. Again, the communication between different clusters is termed as inter cluster communication. Only a subset of nodes called cluster heads participate in the long routing path setup process.

Corresponding Author: C. Vijayakumaran, Research Scholar, Computer Science and Engineering, AISECT University, Bhopal, India.

The unsecured and unprecedented nature of wireless channels provide intruders to inject various malicious attacks to the nodes [2] in order to compromise the network resources. Any secure routing solutions proposed for fixed-infrastructure based wireless networks would not fit well for mobile adhoc networks due to its dynamic nature of topology. Such kind of network creates single point of failure while secure key distribution and key management are the essential requirements for implementing security mechanisms. So, a distributed architecture is required to achieve desired functionalities of secure routing mechanisms used in the MANETs environment.

The MANET architecture can be categorized into two groups: flat and hierarchical. All nodes have equal responsibility and does not scale well in the flat architecture where as large number of nodes can be grouped under clusters based on communication range and location of nodes in the hierarchy based network architecture [3]. Each cluster is managed by a cluster head (C_H) node which can be periodically elected among cluster members by using existing cluster head selection algorithms such as T-LEACH [4] and DHCE [5]. The main role of a cluster head in the network is to act as a coordinator between intra-cluster members as well as inter-cluster heads. The clustering mechanisms provided for MANETs [6-8] can be classified as Secure Clustering approaches and Insecure Clustering approaches. Insecure clustering approaches are not considered here, since the focus of this paper is only on secure clustering approach. Secure clustering approaches are further classified as trust based, cryptographic based and hybrid.

Authentication of nodes is the foremost requirement of secure routing path construction process in any network. With the aid of a centralized authority, authentication of nodes can be easily achieved through existing routing algorithms. However, such a centralized authority is not feasible in adhoc network environment. Hence, the authentication of nodes depends on the trustworthiness of intermediate neighbor nodes in the forwarding path. Outside attacks can be mitigated by using cryptographic based clustering approaches. However, they are unable to detect insider attacks in the network. In order to thwart insider attacks, trustworthiness of nodes is required. Hence, cryptographic approaches can be combined with trust based approach to handle both inside and outside attacks in the network. Existing approaches [9-11] considered several metrics to evaluate the trustworthiness offered by nodes in a cluster. In this work, a dynamic trust model is proposed for evaluating the trust of a node in the route establishment process. It is integrated with our existing approach for trust based coded multicast routing with secure authentication [12].

Network Model: An example of cluster based mobile adhoc network is shown in Figure 1. Each cluster in the network consists of member nodes and a head node. The cluster head node is the most powerful node in a cluster in terms of energy, bandwidth and memory requirements of a node. Each node in the cluster can directly communicate only to its one hop neighbor nodes and its cluster head. In order to communicate with a node in different clusters, multi-hop communication is required. Cluster head provides important role in secure route establishment process. Member nodes exchange security keys with cluster heads to prove their credibility. Frequent key exchange may result in communication overhead. To avoid it, a node should provide its pre-loaded secret key to its cluster head while joining the network. A random generated shared keys between member nodes avoids the malicious nodes in the network region. Freshness of the shared random key is verified by the cluster head to avoid replay attacks.

A logical back-bone network is formed between inner-clusters through cluster heads which can be used to analyze inter-cluster traffic conditions. The existence of back-bone network depends on the life time of inter-cluster heads. Cluster heads have knowledge of its member nodes and keep track of location of member nodes within its geographical region. A node can join or leave a cluster at any time. Hence, the proposed mobile adhoc network architecture enables tangible management of inter and intra cluster routing. Though the routing algorithm used in the network is identical, selection of communication paths between inter cluster and intra cluster is dynamic and it depends on the availability of bandwidth in a specific path. Initially, it is assumed that all nodes in the network are trustable and can share certain cryptographic key parameters for successful key management while establishing a forwarding path. It is also assumed that the C_H knows the location of its member nodes through any existing location tracking and positioning methods [13] since nodes are always movable in the network region. It is assumed that a cluster head may exhibit lesser movement than its member nodes in order to save energy.

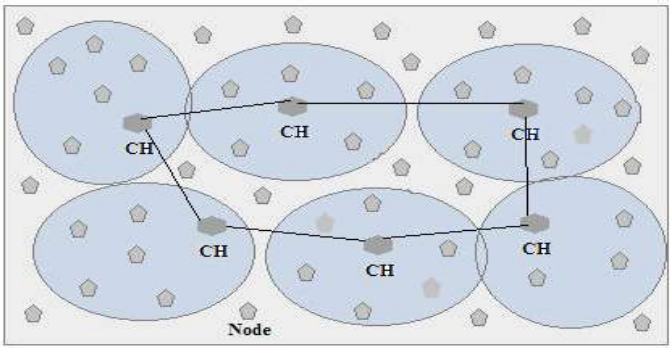

Fig. 1: An example of a cluster based MANET

Trust Model: Due to uncertainty in network topology and inherent unreliable nature of wireless medium, a trust model is necessary in adhoc environment to encounter reputation among the nodes in MANETs. Trust management schemes encompass computation of trustworthiness of a node in forwarding packets in the cluster based network environment [14-15]. The trust can be established in a cluster based on the spatial and temporal information of nodes. However, it may be inaccurate due to network dynamics. Nodes exhibit different levels of trust with respect to their experience with target nodes. Hence, a concrete trust model is required to evaluate the trust of a node inside a cluster. A trust model should consider the network metrics such as packet dropping ratio, packet delivery time, energy and TTL value while evaluating the trustworthiness of a node.

In the proposed work, a cooperative trust establishment approach is used as a trust model in the network. It has two level of trusts: Unswerving Trust (U_T) and Wavering Trust (W_T). The unswerving trust provides direct trust relationship between intra cluster members whereas wavering ftrust provides indirect trust relationship between inter cluster members. A trust weight value (T_w) is assigned with each node in a cluster when it successfully forwards a packet to a destination within the given time. In our previous work [12], authentication of control and data packets are achieved through coded packets and null key packets which are provided by a Certificate Authority (*CA*) whose role is to generate public key certificates. The CA acts as a common trustable authority among cluster heads and responsible for key management and authentication of cluster members. A cluster head can also act as a *CA* if it meets the required trust level as it was fixed by a threshold value. Hence, the distribution of *CA* between the cluster heads avoids single point of failure and enhances the security. Public key certificates are generated by the *CA* and assign it randomly to the cluster heads which in turn negotiates an identity based shared secret keys to its member nodes. Finally, the trust model needs every node to have a trust table for storing its trust value, neighbor's trust value and its encrypted shared secret key exchanged with its neighbor nodes which will be required during the secure route establishment process.

The Cooperative Trust Establishment Approach: The proposed cooperative trust establishment approach has four phases to achieve secure and reliable data forwarding path establishment process in the network.

Intra Cluster Trust Evaluation: The unswerving trust is defined as a direct trust relationship between cluster member nodes that enables a node to believe the capabilities of its neighbor node in forwarding data packets with respect to given trust class. On the other hand, wavering trust shows the indirect relationship between the inter cluster members. It enables a node to believe another node in recommending a trustable third node in the forwarding path while establishing inter cluster communication. The both trust values are changing in time with respect to node movements inside a cluster.

Let U_T represents the unswerving trust between neighbor nodes n_1 and n_2 of a cluster at time t. which can be computed from the equation (1).

$$T_U = 1-(1-U_T)^{Tw}(t) \quad (1)$$

where T_w is the weight assigned to each node at time t. In the proposed trust model, the calculated trust value ranges between 0 to 1. After driving a new trust value (T_U) of a node, a node updates its trust table with the new trust

value and also announces it to its neighbor nodes. The neighbor node adaptively takes decision about trustworthiness of the announced node by comparing it with its old value. If it is greater than the previous value, then the neighbor node updates its trust table to reflect the changes. The unswerving trust can be used in routing path construction between inter cluster members.

Inter Cluster Trust Evaluation: The inter cluster communication involves different nodes and cluster heads based on the distance between a sender in one cluster and a receiver in another cluster.

Let Vi (i= 1 … n) be the set of nodes in the indirect path then the wavering trust (W_T) of the inter cluster routing path can be calculated from the equation (2).

$$W_T = \prod_{i=1}^{n} [1 - (\sum \sqrt{T_U} * T_w)](t) \quad (2)$$

where T_U is the unswerving trust of individual nodes in the path. Then, the calculated trust value is encrypted along with the node's shared random key for secure inter cluster communication.

Secure Intra Cluster Routing: Let us assume that two nodes n_a and n_b are in a cluster and the sender n_a wants to send a packet to the receiver n_b at time t. The secure intra cluster routing process is shown in Figure 2:

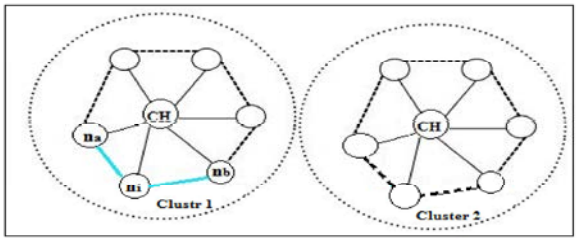

Fig. 2: Secure Intra Cluster Routing Process

The main aim of the secure intra cluster routing approach is to forward a data packet securely from a sender node to a receive node situated in the same cluster. The steps involved in the intra cluster routing is given in the procedure 1.

Procedure 1: Secure Intra Cluster Routing

- The node n_a and n_b already registered as member nodes of a cluster by negotiating their pre-loaded secret key (K_s) with their cluster head (C_H) while they have been joined the cluster.
- Node n_a sends a route request (r_{req}) message to its one hop members with its encrypted shared random key (K_r) and its calculated trust value (T_U).
- After receiving a route reply message (r_{rep}) from any one of its one-hop neighbor(n_i), it verifies the integrity of the received message by applying a hash function F.
- Then, the sender gets the public key certificate from CA (here, C_H) and decrypt the reply message to verify the authentication of the received message.
- Finally, it compares the trust value of the neighbor node from a previous trust value stored in its trust table.
- If the neighbor's trust value is less than the old value, it earmarks a negative flag in its trust table about the neighbor node's reputation in forwarding the packet.
- If it is greater than old value, then the sender updates the new trust value of neighbor in its trust table and forwards the packet to the intermediate node.
- The steps 2-7 are repeatedly applied until a stable route is established between the sender (n_a) and the receiver (n_b). The sender now sends its encrypted data packet to the receiver via the established secure path.
- When the receiver receives the data packet from the sender and decrypt it with it private key, it then sends an encrypted acknowledgement packet (*ack*) in the reverse path.
- If the *ack* packet is not received within the given time t, the sender retransmit the same packet.

In the intra cluster communication scenario, the eavesdropping of nodes is not possible for an attacker due to encryption and integrity verification of the transmitted messages through hash function. Further, the negative flag of an untrusted node avoids intruders in the network.

Secure Inter Cluster Routing: Let us assume that the sender (n_a) and the receiver (n_b) are in different clusters. The secure inter cluster route is established between the sender and the receiver through the intermediate nodes and cluster head nodes (n_1, n_2 and C_H) as shown in Figure 3.

The main aim of the secure inter cluster routing approach is to forward a data packet securely from a sender node in a cluster to a receive node situated in another cluster. The steps involved in the inter cluster routing is presented in the procedure 2.

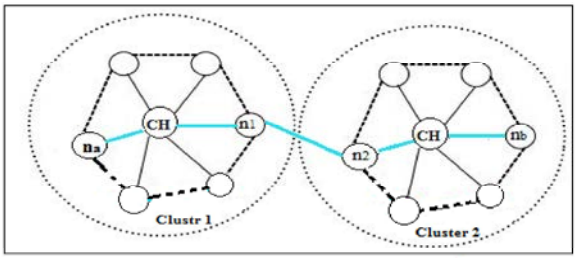

Fig. 3: Secure Inter Cluster Routing Process

Procedure 2: Secure Inter Cluster Routing

- As with the pre-loaded keys, it is assumed that nodes are properly register with their respective cluster heads.
- The sender (n_a) sends a route request and establishes the secure route as in the case of intra cluster communication. However, the intermediate nodes (n_1 and n_2) and the cluster heads (C_Hs)are involved in the secure route establishment process.
- The status of negative flag of each node is checked in each hop and if each node is trusted, a session key is then exchanged to verify the authentication of involving nodes in the route construction process. The integrity of the message can be verified by applying a hash function *F*.
- After establishing a secure path, the sender sends its encrypted data packet with its session key to the receiver through the secured path.
- The receiver gets the public key certificate from its head node and decrypts the incoming packet by using its private key.
- Finally, the receiver sends the encrypted acknowledgement packet (*ack*) in the reverse path.

Again, the attacks from inside and outside of a cluster is mitigated by using the security measures taken in to the account of signing and verifying the packets involved in both types of cluster communications. The authentication of data packet is achieved by using public key certificates. Integrity of the message relies on the hash function *F* used in the above process. The trust relationships between inter cluster members are depending on knowledge of intermediate nodes about the existing trustworthiness of their neighbor nodes. Whenever a node receives new trust value greater than the previous one stored, it updates its neighbor trust table which ensures the freshness of the trusted route.

Each node in the network maintains updated trust table for recording trust values of its neighbor nodes which will be referenced while obtaining a public key certificate from *CA*. The highest trust value is considered during the head node election process. A fake node may try to create high trust value which can be identified by comparing the calculated trust value with a pre-defined threshold value. If it is higher than the threshold value, it will be immediately discarded and the respective node is marked as malicious node. In the multicast routing scenario, a node selects most trustable path among all possible forwarding paths established by the sender.

Performance Analysis: The performance of the proposed work is analyzed by using Network Simulator (NS2) [16] as the simulation tool. The analysis process includes trusted member nodes, non-trusted member nodes and their influence in the evaluation of trust with respect chosen threshold value. In the simulation process, a network consists of 200 nodes with four cluster where each cluster has equally distributed nodes. Initially, each cluster is assigned with a small of malicious nodes percentage (say p) which have been then gradually increased with respect to simulation time. Table 1 shows the details of parameters used in the simulation process. The IEEE 802.11MAC protocol Distributed Coordination Function (DCF) [17] is used as MAC protocol for wireless LAN. The random waypoint mobility model [18] is used to show the mobility of a node from random location to a random destination node at a random speed.

The Figure 4 shows the comparison of packet dropping ratio of malicious nodes of the proposed approach with existing mechanism. The malicious node may perform different kinds of attacks such as gray hole attack, replay attack and also intentionally drop packets. The proposed approach (TICMR) is showing less number of packet drop rate when comparing with existing Trust based Quality Routing (TQR) [19]. Even with the increased number of malicious nodes, the proposed approach still exhibits stability in packet dropping rate due to the trust value is included in the node's trust evaluation process. The cluster radius [20] affects the overall performance of the network. The larger radius of cluster results in high delay in both type of cluster communications. Clusters with moderate radius provide performance gain in the hierarchical key management [21] and shows a balance between good performance and better resilience to security attacks.

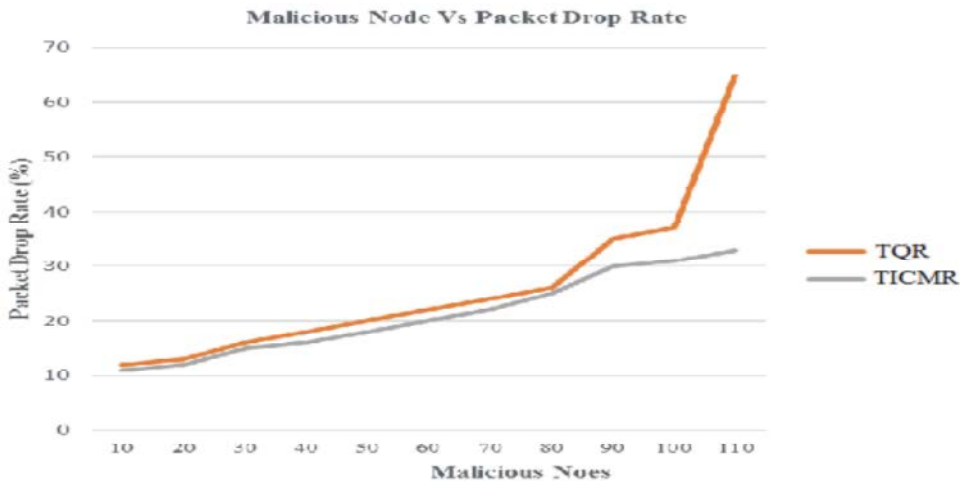

Fig. 4: Packet Dropping rate of Malicious Nodes

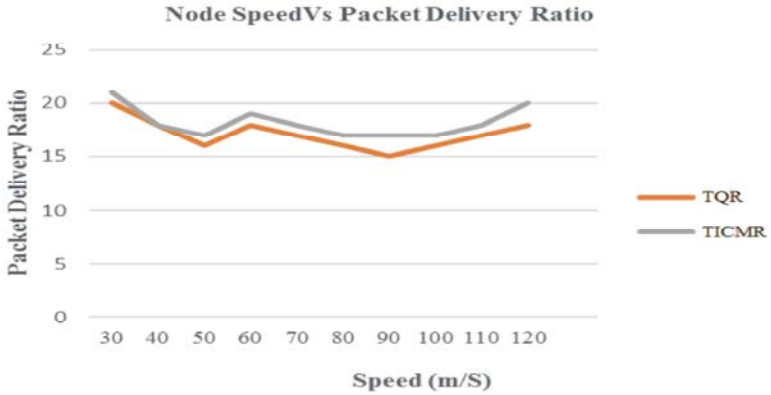

Fig. 5: Packet Delivery Ratio of Mobile Nodes

Table 1: Simulation Parameter

Number of nodes	200
Number of Clusters	4
Network Size	500 m x 500 m
Mobility Model	Random waypoint
Traffic model	CBR
Packet size	512 bytes
Transmission Radius	150 m
Routing Protocol used	DSR/AODV

The performance of the proposed approach in delivery of packet ratio with respect to the mobility of nodes is shown in the Figure 5. The accuracy of trust value calculated in the integrated approach depends on the collaboration of individual nodes in the cluster and it also depends on the trustworthiness of neighbor nodes.

The performance of the proposed TICMR outperforms well in delivering packets with respect to varying speed of mobile nodes. The average packet delivery ratio will be maintained even at high mobility condition of nodes in a cluster.

CONCLUSION

There has been a rapid growth in the applications of mobile adhoc networks in various fields such as battle field, disaster rescue management, environment monitoring and health care monitoring. The collaborative nature of mobile nodes in the network enables the importance of secure multicast routing to prevent attackers and intruders. Trust based intra cluster and inter cluster routing approaches are proposed in this paper to protect clusters against insider attacks as well as outside attacks in the network. From the recommended trust relationship between the mobile nodes, the behavior of malicious nodes can be easily identified and eliminated from the clusters. The proposed approaches mainly focus on integrating the trust based clustering approaches with secure multicast routing to achieve authentication and verification of messages exchanged between mobile nodes and from the simulation results, it could be evident that the integrated trust based clustering approach not only compensate the vulnerabilities of mobile nodes but

also yields better performance in packet delivering ratio than the existing schemes. The key factors that affect the hierarchical key management of cluster heads will be considered in the future work.

REFERENCES

1. Luo, J., D. Ye, L. Xue and M. Fan, 2009. "A survey of multicast routing protocols for mobile Ad-Hoc networks", IEEE Communications Surveys & Tutorials, 11(1): 78-91.
2. Rachedi, A., A. Benslimane, H. Otrok, N. Mohammed and M. Debbabi, 2009. "A Secure Mechanism Design- Based on Game Theoretical Model for MANETs", Mobile Network Application, Springer Science and Business Media, LLC, 6th May, 2009.
3. Banerjee, S. and S. Khuller, 2001. "A Clustering Scheme for Hierarchical Control in Wireless Networks", Technical Report, Department of Computer Science, University of Maryland, College Park, CS-TR-4103-2001.
4. Song, F. and B. Zhao, 2008. "Trust-Based LEACH Protocol for Wireless Sensor Networks", In Proceedings of the Second International Conference on Future Generation Communication and Networking", IEEE Computer Society, Washington, DC, 1: 202-207.
5. Zabian, A., A. Ibrahim and F. Al-Kalani, 2008. "Dynamic head cluster election algorithm for clustered Ad-Hoc networks, " Journal of Computer Science, 4(1): 42-50.
6. Chinara, S. and S.K. Rath, 2009. "A Survey on One-Hop Clustering Algorithms in Mobile Ad Hoc Networks", Journal of Network and Systems Management Archive, 17(1-2): 183-207.
7. Wei, D. and H.A. Chan, 2006. "Clustering Ad Hoc Networks: Schemes and Classifications", 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, pp: 920-926.
8. Yu, J.Y. and P.H.J. Chong, 2005. "A Survey of Clustering Schemes for Mobile Ad Hoc Networks", IEEE Communications Surveys & Tutorials.
9. Golbeck, J., 2006. "Computing with Trust: Definition, Properties and Algorithm, " Workshop on Security and Privacy for emerging Areas in Communication Networks, Baltimore, MD, pp: 1-7.
10. Hamed Samavati, Behrougz Tork Ladani, Hossein Moodi, 2011. "AMLeT: Adaptive Multi Level Trust framework for MANETs", International Symposium on Computer Network and Distributed System (CNDS), February 23-24.
11. Theodorakopoulos and J.S. Baras, 2006. "On Trust Models and Trust Evaluation Metrics for Ad-hoc Networks, " IEEE Journal on selected Areas in Communications, 24(2): 318-328.
12. Vijayakumaran, C. and T. Adiline Macriga, 2014. "Trust based Coded Multicast Routing with Secure Authentication in MANET", International Journal of Applied Engineering Research, 9(24): 27277-27290.
13. Shakhakarmi, N. and D.R. Vaman, 2010. "Distributed Position Localization and Tracking (DPLT) of Malicious Nodes in Cluster Based Mobile Ad hoc Networks (MANET)", WSEAS Transactions in Communications, ISSN: 1109-2742, 9(11).
14. Park, C., Y.H. Lee, H. Yoon, D.S. Choi and S.H. Jin, 2005. "Cluster based trust evaluation in ad hoc networks", In Proceedings of International Conference on Advanced Communication Technology, pp: 503-507.
15. Cho, J.H., A. Swami and I.R. Chen, 2010. "A survey of trust management in mobile ad hoc networks", IEEE Communications Surveys and Tutorials, Dec. 2010.
16. Zhu, Y. and T. Kunz, 2004. "MAODV Implementation for NS-2.26, " Technical Report SCE-04-01, Dept. of Systems and Computing Engineering, Carleton University, January 2004.
17. "Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications 802.11", 1997.
18. Bettstetter, C., G. Resta and P. Santi, 2003. "The node distribution of the random waypoint mobility model for wireless ad hoc networks", IEEE Transactions on Mobile Computing, 2(3): 257-269.
19. Bo Wang, Xunxun Chen and Weiling Chang, 2014. "A light-weight trust-based QoS routing algorithm for ad hoc networks", Elsevier Journal for Pervasive and Mobile Computing, 13: 164-180.
20. Angione, G., P. Bellavista, A. Corradi and E. Magistretti, 2006. "A k-hop Clustering Protocol for Dense Mobile Ad-Hoc Networks", In the Proceedings of the 26th IEEE International Conference on Distributed Computing Systems Workshops (ICDCSW'06), Lisbon, Portugal.
21. Gennaro, R., *et al*., 2008. "Strongly-Resilient and Non-Interactive Hierarchical Key-Agreement in MANETs, " In the Proceedings of the 13th European Symposium on Research in Computer Security (ESORICS '08), Berlin, Heidelberg.