Journal of Computer Science, 9 (2): 147-154, 2013
ISSN 1549-3636

doi:10.3844/jcssp.2013.147.154 Published Online 9 (2) 2013 (http://www.thescipub.com/jcs.toc)

A Hybrid Approach for Node Co-Operation Based Clustering in Mobile Ad Hoc Networks

[1]Sathiyakumar, C. and [2]K. Duraiswamy

Department of Computer Science and Engineering,
K.S. Rangasamy College of Technology,
Tiruchengode-637 215, Namakkal, Tamilnadu, India

Received 2012-07-14, Revised 2012-08-30; Accepted 2013-3-26

ABSTRACT

A Mobile Ad-Hoc Network (MANET) is termed as a set of wireless nodes which could be built with infrastructure less environment where network services are afforded by the nodes themselves. In such a situation, if a node refuses to co-operate with other nodes, then it will lead to a considerable diminution in throughput and the network operation decreases to low optimum value. Mobile Ad hoc Networks (MANETs) rely on the collaboration of nodes for packet routing ahead. Nevertheless, much of the existing work in MANETs imagines that mobile nodes (probably possessed by selfish users) will pursue prearranged protocols without variation. Therefore, implementing the co-operation between the nodes turn out to be an significant issue. The previous work described a secured key model for ad hoc network with efficient node clustering based on reputation and ranking model. But the downside is that the co-operation with the nodes is less results in a communication error. To enhance the security in MANET, in this work, we present a hybrid approach, build a node co-operation among the nodes in MANET by evaluating the weightage of cooperativeness of each node in MANET. With the estimation of normal co-operative nodes, nodes are restructured on its own (self). Then clustering is made with the reorganized nodes to form a secured communication among the nodes in the MANET environment. The Simulation of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) work is done for varying topology, node size, attack type and intensity with different pause time settings and the performance evaluations are carried over in terms of node cooperativeness, clustering efficiency, communication overhead and compared with an existing secured key model. Compared to an existing secured key model, the proposed HANCC performance is 80-90% high.

Keywords: MANET, Node Cooperativeness, Hybrid Approach, Clustering, Self-Organization

1. INTRODUCTION

Mobile Ad hoc Networks (MANETs) are illustrious from further communication networks by numerous features. The primary portion is that, mobile nodes in MANETs might progress generously in the nonexistence of a predetermined infrastructure. Consequently, regular alterations in routes may take place due to changeable topology transform and link disconnections. The next process, nodes in MANETs has restricted resources such as bandwidth, energy and computational authority. At last, MANETs have no expected central influence. Therefore, security mechanisms should be dispersed and should not origin unnecessary resource utilization. However, MANETs have an extensive range of military and marketable applications.

Mobile Ad hoc Networks (MANET) have drained widespread consideration in current years due to the growing demands of its prospective applications. In conventional crisis or military situations, the nodes in a MANET frequently fit into the similar ability and perform considerately for the general goals. In recent times, promising applications of MANETs are also visualized in resident usage, where nodes classically do

Corresponding Author: Sathiyakumar, C., Department of Computer Science and Engineering, K.S. Rangasamy College of Technology, Tiruchengode-637 215, Namakkal, Tamilnadu, India

not fit into a solitary ability and may not follow a general goal. We submit to such networks as self-organized (self-organized) MANETs. Before MANETs can be effectively organized in a self organized way, the concern of cooperation inspiration must be determined.

MANETs are classically self-organized networks and transitional nodes should transmit the continuous communication. To attain this, each node relies on its neighbor to promote the packet to the intention. In fact, most of preceding revises on MANETs has absolutely unspecified that nodes are supportive. As such, the concern of node cooperation becomes very imperative in MANETs. Nevertheless, cooperation may be harder to implement in MANETs than in communications based networks owing to numerous reasons. At initial stage, nodes can subjectively connect or depart the network. Second, recognition of naughtiness and consequent separation of a misbehaved node has to effort in a dispersed method owing to lack of central control. At last, user precise requirements or approach should not be overlooked. Some users observe their power resource as being restricted by battery life and consequently they may not believe disposed to transmit track for other users. As such, user's performance will blow the system performance determined by his relevance needs or substantial constraints.

In common, awkward nodes in MANETs may be classified into two modules: Malicious nodes and selfish nodes. The phrase malevolent refers to the collection of nodes that purposely try to assail the system or smash the network. Alternatively, the name selfish identifies the nodes so as to endeavor to increase help from the network without disposed to compensate back the help established. Both malicious and selfish nodes are measured as misbehaving nodes.

In this study, we are going to present a weightage scheme for cooperativeness of each node in the MANET environment. After evaluation of weightage scheme, self-organization of node is done and then the clustering is made for a secure communication.

1.1. Literature Review

Mobile Ad hoc Networks (MANETs) are renowned from further communication networks by several features. First, portable nodes in MANETs may progress liberally in the nonexistence of a permanent infrastructure. Cooperation among nodes is vital for the operationally of a Mobile Ad-hoc Network (MANET). Since a MANET is frequently organized in uninhibited environments, some nodes might be negotiated by an opponent and bound for to act spitefully. The author (Natarajan *et al*., 2012) presented scalable trust management system to partition and amass in sequence network of belief metadata of nodes in a MANET. Nevertheless, as the nodes in a MANET are usually resource restricted, some nodes might decline service to other nodes to preserve their resources, thus showing selfish behavior. At last, MANETs have no faith central ability. To tackle this problem, we offer a reputation-based system (Zhang *et al*., 2011a) for DTNs to diminish the destruction fetched by selfishness. A procedure of collection ahead and a method of activities recording are offered for the discovery of misbehaving.

All the nodes perform sensibly to split their possessions for the comprehensive connectivity and might simply be weakened in the existence of self-seeking individuals. To deal with this problem, (Zhang *et al*., 2011b) proposed a cooperation enforcement scheme based on reputation. To improve the throughput and reduce the delay time of the network, (Fu *et al*., 2012) presented a cooperative approaches beneath congregate cast for both static and Mobile Ad hoc Networks (MANETs), correspondingly. At first, it initiate a common concept of reputation to distinguish and enumerate the mesh node's behavior/status in terms of fine-grained presentation metrics. Current years, researchers have planned several positioning algorithms for wireless sensor networks (Mishra, 2009). Xu *et al*. (2010) proposed a Reputation-based Revising Scheme (RRS) to access the unrefined localization information before pertaining any positioning algorithm.

In multi-hop networks for instance Mobile Ad hoc Networks (MANETs), a node can behave badly by falling others' packets to accumulate battery life. This self-centeredness or misbehavior can interrupt the entire network functionality. To progress this, reputation based schemes are utilized for preventing white wash attacks (Abbas *et al*., 2010). To improve the security in MANET (Rong *et al*., 2009) is planned to implement a pyramidal security form to preserve the multi security-level information distribution in one assistance domain. It is exclusively supported on each node's possess past actions and its personal defective examination of other nodes' information. Li and Liu (2010) presented a method for a secure communication utilizing group key management protocol. It used ID supported confirmation key for a safe communication over ad-hoc network. An encryption technique (Sumathy and Kumar, 2010) is utilized for a safe key substitute over the nodes in the network.

A cooperation enforcement (Ji *et al*., 2006; 2010) in independent mobile ad hoc networks under sound and

defective examination and revise the high performance collaboration among the nodes (Cai and Li, 2010) using the Projection Pursuit based risk assessment with defective information based on node cooperation (Wang *et al*., 2008). The safe communication is completed based on node cooperativeness in this work by clustering according to it.

2. MATERIALS AND METHODS

The proposed work is efficiently designed for enhancing a secure communication over MANET by improving the node cooperativeness among the nodes in the network. The proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) comprises of three operations. The first process is evaluating the weightage scheme of cooperativeness in the system. The second process is after evaluation; the self organization of node is done. The third process is to cluster the nodes based on weightage scheme and self organization for a secure communication. The architecture diagram of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) is shown in **Fig. 1**.

The first process is to evaluate the cooperativeness of each node in the MANET. The evaluation of cooperativeness is done based on the behavior and activities of the node done while the communication is taking place between the nodes. The monitoring of the behavior of the nodes is carried out and based on that the cooperativeness of the nodes is assumed. The weightage of the cooperativeness of each node is computed based on the spatial events occurred at different aspects of communication takes place.

The second process is self organization of nodes takes place once after a completion of computing the cooperativeness of the nodes. With the evaluation of normal co-operative nodes, clustering of node is reorganized on its own (self). It does not allow any unauthorized node to involve in the communication between the nodes in ad-hoc network.

The third process is to cluster the nodes based on weightage scheme and the organization of nodes to provide a secure communication to the users involved in MANET environment.

2.1. Evaluation of Weightage of Node Cooperativeness

We present a new scheme that implements node cooperation in MANETs.

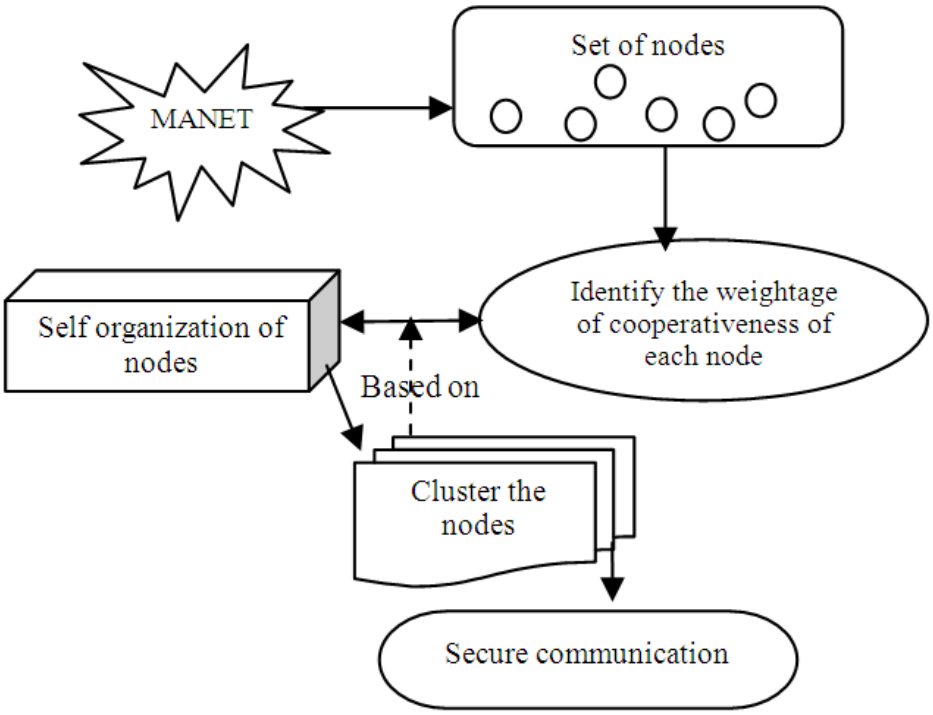

Fig. 1. Architecture diagram of the proposed HANCC

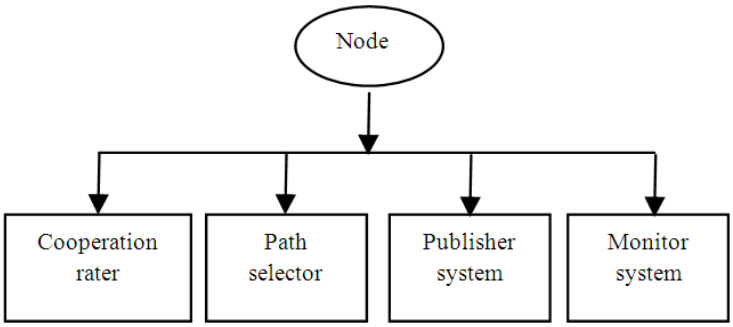

Fig. 2. Computing node cooperativeness

The cooperation rater consists of

Node ID	My count	Node total help	N or F

Fig. 3. Components of cooperation rater

Recall that virtual currency schemes provide more fairness and the collaboration among nodes in reputation-based schemes is better. When a node comes into a new region of VGA, it transmits a message to recognize itself to the node in that region and to identify the neighboring nodes. Therefore, a node can recognize its neighbors. The model is constructed on Dynamic Source Routing (DSR) which in turn functions on top of VGA. In addition to this, each node in the network supports one of four categories of Reputation values (R). These are:

- New node: when a new node enters into the network for the first time, it is consigned an initial value that is equal to 0
- Normal node: a supportive node that has a reputation value R where 0<R<Ts
- Super node: A supportive node that has a reputation value R where R>Ts
- Misbehaving node: A self-centered node that have a reputation value R where R<Tm

where, Ts and Tm are an edge values for super cooperative and misbehaving nodes, correspondingly. Note that the super node is desired to designate those nodes that will cooperate much more dynamic role than others as of their location with regard to other nodes.

In MANET, all nodes are conscious of the activities of all other nodes. Each node supervises the activities of its neighbor using a straight examination and a legitimate reputation message. Each node sustains a table that explains the activities of each of its neighbors. Each record in the table illustrates one neighbor and encloses information concerning this neighbor for instance its Total Help (TH) that was offered to further nodes in the network. When a source node A begins its session during a route of intermediary nodes, the first transitional node forwards the packet and all neighbor nodes increase the TH field associated to it by a value of one and at the similar time decrement the TH for node A based on the acknowledgment of the packet which is sent. If the intermediate node declines the packet, its TH is decreased by a value of two. This procedure will pertain to all nodes contributing in the forwarding function. Each node in the MANET needs to identify the weightage of cooperativeness with other nodes. The node cooperativeness is computed as shown in **Fig. 2**.

Cooperation rater preserves a data structure that illustrates the activities of its neighbors and some distant nodes. Each record in the table comprises the subsequent information. The components of the cooperation rater is shown in **Fig. 3**:

- Node ID: Unique identifier of each node
- My Count: Represents the quantity of help given - help received by the node
- Node Total Help: Total help a node provided to its neighbors
- N or F: Represents the neighbor (one-hop) node, correspondingly

If there are several routes among the source and the destination, then the Path Selector will choose the path that has fewer probabilities for removing the packet. The Publisher System traces the ranking of the neighboring nodes. The Publisher System also practices all arriving reputation message in a definite node. Monitor system observes the activities of its neighbors and reports to the Cooperation Rater. Using the cooperative rater, the cooperativeness of the nodes is computed reliably.

```
Input: Set of nodes N, message M
Step 1: For each node N
Step 2:    Assign node Id
Step 3:    Identify the quantity of node
Step 4:    Monitor the activities (B) of the node
Step 5: End For
Step 6: Note the path (P) chosen by the node from
        the beginning
Step 7: Note the total help (TH) provided by the
        node N
Step 8: Based on P, TH, B
Step 9:    Compute the weightage of
           cooperativeness (WC)
Step 10: End
Step 11: Based on WC,
Step 12:    Reorganize the nodes in the MANET
Step 13:    Cluster the nodes
Step 14:    If WC (node) has max. Value
Step 15:       Assign it as Cluster Head
Step 16:       Cluster head manage the group by
               forming a nodes which has better
               WC
Step 17:       Form a group
Step 18:    End if
Step 19: End
```

Fig. 4. Pseudo code of HANCC

2.2. Process of Self-Organization and Node Clustering Based on Cooperativeness

After completion of computing the node cooperativeness, the self organization of nodes in MANET takes place. Since the node cooperativeness weightage is processed based on the activities, now the network environment consists only of true nodes by discarding the selfish nodes which involved in node attack, message lost and so on.

The clustering of node is done based on the cooperativeness weightage. The clustering process is done based on the nodes which have high cooperativeness weightage and acts as a Cluster Head (CH). After assigning the cluster head, the CH will manage to group the nodes based on the cooperativeness weightage matched with it. Then the communication takes place among the nodes based on clustered value. The process of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) is described here with pseudo code (**Fig. 4**).

The process of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) is described elaborately in **Fig 4**. For each node in the MANET, it is necessary to assign a node ID and to monitor the activities of the node. The path chosen by the node is also being noted to identify whether the node follows correct path to transmit a message. Then identify the node whether it can adjust with the behavior of other nodes in the network. After computing the weightage of cooperativeness, the reorganization of node takes place. Clustering is done based on the cooperativeness value and found the cluster head to form a cluster group to provide a secure communication for the nodes involved.

3. RESULTS

The proposed node cooperativeness estimation based clustering is efficiently done through evaluating the cooperative rater. To estimate the performance of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC), we run simulations on a Linux machine, having a P4-3.4 GHz processor with 2 GB of memory. We implement the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) into an NS-2 environment. The simulation area extents 900×900 m^2, in which nodes can move from a random starting point to a random destination, with speeds of 3, 6, 9 m sec^{-1} and a pause time of 3-5 sec. At first, the nodes cooperativeness is first identified based on the behavior and activities of the nodes in the network environment, after evaluating the cooperativeness value, the nodes are reorganized in a same way. Then the node clustering is done based on the maximum value obtained by the node in cooperativeness range. Since the node clustering is performed based on weightage of cooperativeness scheme, the clustering process will be an efficient one. Then the communication among the nodes is also being good compared to an existing secured key model framework. The performance of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) is measured in terms of Node cooperativeness, clustering efficiency, Communication overhead.

Node cooperativeness describes the cooperativeness of the nodes in the network. The table (**Table 1**) describes the cooperativeness of the nodes after applying the appropriate method. The results of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) is compared with an existing secured key model.

Figure 5 describes the cooperativeness range of the nodes in the network when number of nodes increases. In the proposed HANCC, the node cooperativeness range is detected based on the behavior and activation of the node done till the communication with the other nodes takes place. Since the node cooperativeness is easily detected, the proposed HANCC supports a secure communication to transmit a packet from source to destination.

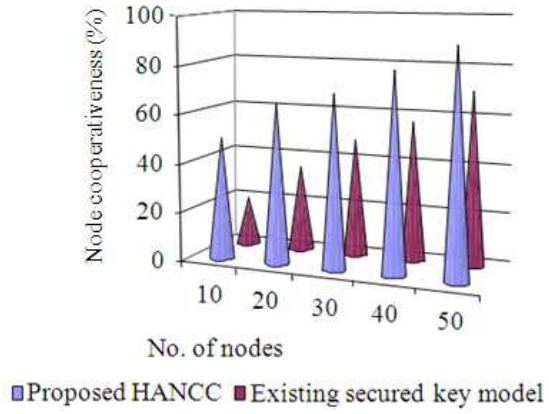

Fig. 5. No. of nodes Vs. Node cooperativeness

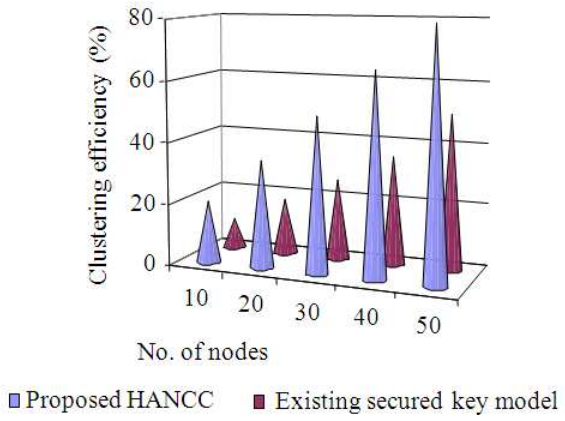

Fig. 6. No. of nodes Vs. clustering efficiency

Table 1. No. of nodes Vs. node cooperativeness

	Node cooperativeness (%)	
No. of nodes	Proposed HANCC	Existing secured key model
10	50	20
20	65	35
30	70	48
40	80	57
50	90	70

Table 2. No. of nodes Vs. clustering efficiency

	Clustering efficiency (%)	
No. of nodes	Proposed HANCC	Existing secured key model
10	20	10
20	35	18
30	50	26
40	65	35
50	80	50

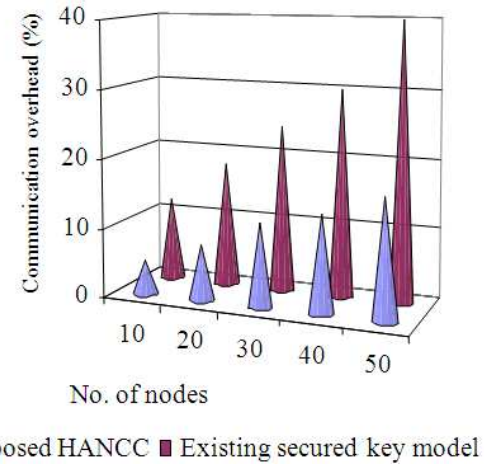

Fig. 7. Clustered nodes Vs. Communication overhead

Table 3. Clustered nodes Vs. Communication overhead

	Communication overhead	
Clustered nodes	Proposed HANCC	Existing secured key model
10	5	12
20	8	18
30	12	24
40	14	30
50	17	40

The node cooperativeness is measured in terms of cooperativeness range (%). Compared to an existing secured key model which has been concerned only for the secure communication, if more number of misbehave node enters, the existing work is abandoned, the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) outperforms well and the variance is 30-40% high in the proposed HANCC.

Clustering efficiency measures the effectiveness of cluster in the network. The table (**Table 2**) describes the efficiency of clustering of the nodes after applying the appropriate method. The results of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) is compared with an existing secured key model.

Figure 6 describes the efficiency of cluster when more number of nodes increases in the network environment. Since in the proposed HANCC, the node clustering is done based on the node cooperativeness range, the clustering efficiency is high. The node which has high cooperativeness range acts as a cluster head and the job of cluster head is to form a group based on weightage of cooperativeness range. The clustering efficiency is measured in terms of how the cluster group will process without allowing the

misbehave nodes. Compared to an existing secured key model, the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) provides an efficient clustering process and the variance is 40-50% high in the proposed HANCC.

Communication overhead, the table (**Table 3**) describes the communication overhead arise based on the clustering efficiency. The results of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) is compared with an existing secured key model.

Figure 7 describes the efficiency of communication based on clustered nodes in the network environment. The communication overhead arise less in the proposed HANCC, since it followed the clustering process based on the cooperativeness range, the communication between the nodes in the network is high compared to an existing secure key model.

4. DISCUSSION

From this study, we have seen that how a secure communication is done based on the weightage of node cooperativeness range. Compared to an existing secured key model which runs under reputation and ranking model leads to a loss of packet at some situation, the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) outperforms well even when attacker rate is high. The table and graph below describes the performance of the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC).

At last, it is being observed that the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) efficiently provide a communication framework among the nodes in the network in a secure manner by evaluating the nodes cooperativeness range.

5. CONCLUSION

In this study, we have efficiently proposed a secured communication framework between the nodes in the network without any loss of data. Since the proposed work is based on the node cooperativeness range, the chance of loss of message is less. After estimating the cooperativeness range of each node, the reorganization of nodes takes place in its own. Then the clustering of node is carried out efficiently and chosen the CH for enhancing the good transmission over the network. In order to enhance the lifespan of the network, node cooperativeness range is computed. Depends upon the range, the clustering and communication would takes place. Consequently, not only the malevolent nodes are discarded, which represent node attack and communication failure, but this also point to exceed the packet data in an efficient manner. The experimental results showed that the proposed Hybrid Approach for Node Cooperation based Clustering (HANCC) perform well in a secure communication over the nodes in the network compared to an existing secured key model.

6. REFERENCES

Abbas, S., M. Merabti and D. Llewellyn-Jones, 2010. Deterring whitewashing attacks in reputation based schemes for mobile ad hoc networks. IFIP Wireless Days. DOI: 10.1109/WD.2010.5657719

Cai, F. and Z. Li, 2010. A projection pursuit based risk assessment method in mobile ad hoc networks. Proceedings of the International Symposium on Intelligence Information Processing and Trusted Computing, Oct. 28-29, IEEE Xplore Press, Huanggang, pp: 60-66. DOI: 10.1109/IPTC.2010.169

Fu, L., Y. Qin, X. Wang and X. Liu, 2012. Throughput and delay analysis for convergecast with MIMO in wireless networks. IEEE Trans. Parallel Distributed Syst., 23: 768-775. DOI: 10.1109/TPDS.2011.194

Ji, Z., W. Yu and J.K.R. Liu, 2006. Cooperation enforcement in autonomous MANETs under noise and imperfect observation. Proceedings of the 3rd Annual IEEE Communications Society on Sensor and Ad Hoc Communications and Networks, Sept. 28-28, IEEE Xplore Press, pp: 460-468. DOI: 10.1109/SAHCN.2006.288502

Ji, Z., W. Yu and J.K.R. Liu, 2010. A belief evaluation framework in autonomous MANETs under noisy and imperfect observation: Vulnerability analysis and cooperation enforcement. IEEE Trans. Mobile Comput., 9: 1242-1254. DOI: 10.1109/TMC.2010.87

Li, L.C. and R.S. Liu, 2010. Securing cluster-based ad hoc networks with distributed authorities. IEEE Trans. Wireless Commun., 9: 3072-3081. DOI: 10.1109/TWC.2010.080610.090759

Mishra, A.K., 2009. Analysis of Secure Routing Scheme for MANET. Department of Computer Science Engineering and Technology.

Natarajan, V.K., S. Zhu, M. Srivatsa and J. Opper, 2012. Semantics-aware storage and replication of trust metadata in mobile ad-hoc networks. Proceedings of the IEEE 26th International Conference on Advanced Information Networking and Applications, Mar. 26-29, IEEE Xplore Press, Fukuoka, pp: 376-383. DOI: 10.1109/AINA.2012.89

Rong, B., H.H.H. Chen, Y. Qian, K. Lu and R. Qingyang *et al*., 2009. A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study. IEEE Trans. Vehicular Technol., 58: 398-408. DOI: 10.1109/TVT.2008.923666

Sumathy, S. and B.U. Kumar, 2010. Secure key exchange and encryption mechanism for group communication in wireless ad hoc networks. Int. J. Applic. Graph Theory Wireless Ad Hoc Networks Sensor Networks 2: 9-16. DOI: 10.5121/jgraphhoc.2010.2102

Wang, K., M. Wu and S. Shen, 2008. A trust evaluation method for node cooperation in mobile ad hoc networks. Proceedings of the 5th International Conference on Information Technology: New Generations, Apr. 7-9, IEEE Xplore Press, Las Vegas, NV., pp: 1000-1005. DOI: 10.1109/ITNG.2008.43

Xu, X., H. Jiang, L. Huang, H. Xu and M. Xiao, 2010. A reputation-based revising scheme for localization in wireless sensor networks. Proceedings of the IEEE Wireless Communications and Networking Conference, Apr. 18-21, IEEE Xplore Press, Sydney, NSW, pp: 1-6. DOI: 10.1109/WCNC.2010.5506661

Zhang, X., X. Wang, A. Liu, Q. Zhang and C. Tang, 2011a. Cooperation enforcement scheme based on reputation for delay tolerant networks. Proceedings of the International Conference on Computer Science and Network Technology, Dec. 24-26, IEEE Xplore Press, Harbin, 4: 2372-2376. DOI: 10.1109/ICCSNT.2011.6182449

Zhang, X., X. Wang, A. Liu, Q. Zhang and C. Tang, 2011b. Reputation-based scheme for delay tolerant networks. Proceedings of the International Conference on Computer Science and Network Technology, Dec. 24-26, IEEE Xplore Press, Harbin, pp: 974-978. DOI: 10.1109/ICCSNT.2011.6182124