American Journal of Applied Sciences 9 (8): 1283-1289, 2012
ISSN 1546-9239

Mobile Anonymous Trust Based Routing Using Ant Colony Optimization

[1]R. Kalpana and [2]N. Rengarajan
[1]Department of CSE,
Vivekanandha Institute of Engineering and Technology for Women, Tiruchengodu, India
[2]K.S.R. College of Engineering, Tiruchengodu, India

Aproach: Problem statement: Ad hoc networks are susceptible to malicious attacks through denial of services, traffic analysis and spoofing. The security of the ad hoc routing protocol depends upon encryption, authentication, anonymity and trust factors. End-to-end security of data is provided by encryption and authentication, topology information of the nodes can be obtained by studying traffic and routing data. This security problem of ad hoc network is addressed by the use of anonymity mechanisms and trust levels. Identification information like traffic flow, network topology, paths from malicious attackers is hidden in anonymous networks. Similarly, trust plays a very important role in the intermediate node selection in ad hoc networks. Trust is essential as selfish and malicious nodes not only pose a security issue but also decreases the Quality of Service. **Approach:** In this study, a routing to address anonymous routing with a trust which improves the overall security of the ad hoc network was proposed. A new approach for an on demand ad-hoc routing algorithm, which was based on swarm intelligence. Ant colony algorithms were a subset of swarm intelligence and considered the ability of simple ants to solve complex problems by cooperation. The interesting point was, that the ants do not need any direct communication for the solution process, instead they communicate by stigmergy. The notion of stigmergy means the indirect communication of individuals through modifying their environment. Several algorithms which were based on ant colony problems were introduced in recent years to solve different problems, e.g., optimization problems. **Results and Conclusion:** It is observed that the overall security in the network improves when the trust factor is considered. It is seen that non performing nodes are not considered due to the proposed ACO technique.

Key words: Ad hoc network, anonymous networks, trust and reputation, security, ant colony optimization

INTRODUCTION

Mobile ad-hoc network is the new paradigm of wireless communication, with a collection of two or more wireless devices enabled to communicate with other nodes within its radio range. Conventional wireless mobile communications use a fixed wire/wireless infrastructure whereas ad-hoc networks are not supported by any fixed infrastructure; it is a self-configuring network of nodes interconnected by wireless links and is defined in IEEE 802.11 standards. The nodes act as both host and routers (Mohapatra and Krishnamurthy, 2005). The nodes communicate in single hop or multi-hop paths with the intermediated nodes acting as routers. Due to the potential mobility of the nodes, the topology of the network is dynamic with addition or deletion of nodes. The infrastructure-less, dynamic and broadcast nature of ad-hoc networks are prone to malicious traffic analysis. Neighbors could be friendly or hostile; information sent in an ad-hoc route must be protected in some way to ensure security and anonymity of exchanged information (Sabari and Duraiswamy, 2009). Providing security and privacy in mobile ad hoc networks has been a major issue over the last few years. Most research work has so far focused on providing security for routing and data content. Anonymous routing is a value-added technique used in mobile ad hoc networks for the purposes of security and privacy concerns. It has inspired lot of research interest, but very few measures exist to trust-aware routing for anonymity protection (Suresh and Duraiswamy, 2011).

The security of the ad hoc routing protocol mainly depends upon encryption, authentication, anonymity and trust factors. While encryption and authentication provides end-to-end security mechanisms of data, information regarding nature and location of the nodes

Corresponding Author: R. Kalpana, Department of CSE, Vivekanandha Institute of Engineering and Technology for Women, Tiruchengodu, India Tel: +91 9486056319

can be obtained by studying traffic and routing data (Asokan *et al*., 2007). This security problem of ad hoc network is addressed by the use of anonymity mechanisms and trust levels.

Most of the routing protocols are based on naïve trust model, where nodes inherently trust all the nodes. Thus it is easy for a malicious node to attack the network by inserting incorrect routing information, erroneous routing update or resending old messages. Security and robustness of the protocol is improved if the a trust based framework is included. The trust is generally quantified using route trust metric and node trust metric (Gopalakrishnan and Uthariaraj, 2011). A trust-based framework evaluates route dependability, identifies and isolates any malicious nodes in the network. Works in literature (Sun *et al*., 2006) provide general frameworks for trust establishment in the network.

The anonymous networks mask various components of the network communication in bid to increase the privacy of communication and also repel intrusions and attacks. The identification information like traffic flow, network topology, paths is concealed in anonymous network for not only a malicious node but also with other valid node (Boukerche *et al*., 2004). Ad hoc routing protocols with anonymity measures protect the privacy of nodes and also check the information flow by malicious nodes. Address spoofing, traffic analysis and certain Denial of Service (DoS) attacks can be prevented in anonymous network by concealing the true identity of the traffic. Many a number of anonymous routing protocols have been proposed in literature (Kong and Hong, 2003).

The attacks on ad hoc network are in form of passive, active attacks and denial of service. Traffic analysis is one of the most subtle passive attacks; an attacker observes network traffic and surmises sensitive information of the applications of underlying system (Guan *et al*., 2001). The leakage of sensitive information could create havoc in security sensitive situations. Active attacks involve malicious actions against node generally after performing traffic analysis. Active attacks involve replication, modification or deletion of data with the intention to degrade or prevent message flow between nodes. Denial of Service (DoS) attacks occurs when the nodes are overloaded with useless traffic by the attacker which leads to the legitimate requests not being processed. Thus, to prevent such kinds of attack and to preserve anonymity of nodes in network, anonymous secure communication is necessary.

Literature review: Netrvalova and Safarik (2009) deal with the interpersonal trust modeling. Terms such as trust, trust values, trust affecting factors and representation of interpersonal trust and its implementation are presented. The proposed trust model tries to integrate more factors which affect trust for trust determination than usual. The model covers basic factors as reciprocal trust, initial trust, subject reputation, number of subject recommendations, number of mutual contacts and trusting disposition. The significance of these factors participating in trust forming is discussed. The interpersonal trust model behavior is examined by a number of parameter studies. The study developed interpersonal trust model integrating factors influencing trust evolution. The experiments proved its behavior to be in accordance with models considering particular factor or subset of factors in our model. Model provides trust formation reasonably sensitive to parameters in proposed formula.

Shao and Huang (2008) proposed a reliable anonymous MANET routing protocol in the sense that the communicating parties are capable of choosing a secure end-to-end route free of any untrustworthy node during the anonymous route discovery process. The key features of the proposed protocol are including of accomplishment of anonymity-related goals, trust-aware anonymous routing, effective pseudonym management and lightweight overhead in computation, communication and storage. The proposed method has efficient solutions to trust-aware anonymity for the route discovery and hence for subsequent data forwarding using the reliable route. It is important to exclude untrustworthy nodes to participate anonymous communications in which all involved nodes nose out malicious attacks hardly. The proposed scheme provides a better tradeoff between security and performance.

Nekkanti and Lee (2004) proposed a routing protocol that is based on securing the routing information from unauthorized users. The proposed routing algorithm basically depends upon the trust one node has on its neighbor. The trust factor and the level of security assigned to the information flow decide what level of encryption is applied to the current routing information at a source/intermediate node. So based on level of trust factor, the routing information will be low-level, medium level, high level encrypted, the low-level being normal AODV. This not only saves the node's power by avoiding unnecessary encoding, but also in terms of time. So, instead of using the same kind of encryption for all the information exchanged, the proposed protocol provides a way to limit this kind of high level of encryption to only the applications which really need them. The decrease in energy consumption to a certain degree is also shown. The proposed protocol could be easily combined with other

routing protocols, e.g., to detect a malicious node and can be implemented in normal civilian networks to high level security military networks.

Chen *et al*. (2010) proposed a novel anonymous routing protocol that provides improved anonymity and security while achieving similar or better performance, as compared to existing proposals. The proposed test aims and achieves anonymity using a novel efficient solution for invisible implicit addressing based on keyed hash chain and security via a novel application of one-to-many Diffie-Hellman mechanism, used to exchange keys for symmetric encryption. The novel anonymous routing protocol for MANETs proposed by the study has shown that it provides both anonymity of sender, receiver and intermediate nodes and data unlink ability in regards to internal and external adversaries. The protocol is also resilient to a wide range of attacks, such as eavesdropping, identity and link spoofing, replay attack and man-in-the-middle attack. Protocol evaluation, done both analytically and using simulation, shows that this protocol provides the smallest control message overhead and compares well to the existing protocols in regards to the stability of routes and latency.

Boukerche *et al*. (2004) proposed a novel distributed routing protocol which guarantees security, anonymity and high reliability of the established route in a hostile environment, such as ad hoc wireless network, by encrypting routing packet header and abstaining from using unreliable intermediate nodes. The proposed protocol allows trustworthy intermediate nodes to participate in the path construction protocol without jeopardizing the anonymity of the communicating nodes. The main features of the proposed protocol include (i) Non-source-based routing (ii) Flexible and reliable route selection and (iii) Resilience against path hijacking has been highlighted.

El Defrawy and Tsudik (2008) focused on the privacy aspect of mobility and proposed a routing protocol, PRISM, which achieves privacy and security against both outsider and insider adversaries. Unlike most networks, where communication is based on long-term identities (addresses), the location-centric communication paradigm is better-suited for privacy in suspicious MANETs. Simulation results compare PRISM with an alternative location-centric link-state approach and show that PRISM generally achieves better performance under reasonable communication assumptions. The results reveal that PRISM is more computationally efficient and offers better privacy than prior work.

Zou and Chigan (2009) proposed a novel Anonymous on Demand Source Routing (AODSR) protocol, which is a scalable distributed solution to achieve sender, receiver and sender-receiver relation anonymity in MANETs. In AODSR, the route discovery process is not controlled by the initiator/target node, but by a series of random residual hop numbers. This not only eliminates the different protocol behaviors of the initiator/target node and intermediate nodes, it also avoids the flooding of routing packets. With the aid of the “buddy” group strategy, the anonymity is further reinforced. Theoretical analysis and simulation shows that AODSR achieves high degree of anonymity while requiring low computational complexity and communication overhead. By controlling the change tendency of the random residual hop numbers, AODSR can avoid routing packets flooding all over the network. This is because the route request autonomously stops when this number decreases to zero. The analysis and simulation concurs that AODSR is a scalable routing protocol of high degree of anonymity with low communication cost suitable for MANETs.

Zhang *et al*. (2005) proposed a novel anonymous on-demand routing protocol, termed MASK, which can accomplish both MAC-layer and network-layer communications without disclosing real IDs of the participating nodes under a rather strong adversary model. To thwart passive eavesdropping and the resulting attacks, MASK offers the anonymity of senders, receivers and sender-receiver relationships in addition to node unlocatability and untrackability and end-to-end flow untraceability. It is also resistant to a wide range of attacks. Detailed simulation studies have shown that MASK is highly effective and efficient. With regard to future research the team proposes to incorporate some intrusion detection capabilities into MASK to defend against not only passive attacks but also active DoS-type attacks such as those mounted on neighborhood authentication. In addition, they also plan to combine MASK with other secure routing protocols to ensure both routing anonymity and strong routing security.

Yang *et al*. (2006) proposed a novel technique to address the issue of an on demand routing protocol at a reduced cost. The proposal dubbed Discount ANODR is built around the same set of techniques as ANODR. The proposed protocol has the benefit of achieving lower computation and complexities at the cost of slight reduction of privacy guarantees. A route is blindly generated by the intermediaries on the path between an anonymous sources and an identified destination. Route requests in Discount ANODR bear strong similarities to route requests in existing source routing protocols with the limitation that only

intermediaries only know the destination of the request and the identity of the previous intermediary. The communication of data uses such route onions to channel the packet to the intended destination.

Boukerche *et al*. (2005) proposed a novel distributed routing protocol which guarantees security, anonymity and high reliability of the established route in a hostile environment, such as ad hoc wireless network, by encrypting routing packet header and abstaining from using unreliable intermediate node. The new protocol titled SDAR creates routes dynamically to support onion routing without the originator knowing neither the keys of the mix nodes nor the topology of the network. It also provides adequate security/anonymity for both sender and receiver during path establishment. This has several advantages compared to previous schemes which are non-source-based routing-source node does not need to know global topology and link availability; route computation shared among many nodes; easy adaptability to changes in network topology; flexible and reliable route selection-route selection is based on the source node's trust requirement to the route and done in a distributed way in the path discovery phase according to intermediate nodes' own direct experience with its neighbor; and resilience against path hijacking-resilience against malicious nodes compromising the communication through collusion

Zhang *et al*. (2006) proposed a novel Anonymous and Certificateless Public-Key Infrastructure (AC-PKI) for ad hoc networks. AC-PKI enables public-key services with certificateless public keys and thus avoids the complicated certificate management inevitable in conventional certificate-based solutions. To satisfy the demand for private keys during network operation, the experiment employs a secret-sharing technique to distribute a system master-key among a preselected set of nodes, called D-PKGs, which offer a collaborative private-key-generation service. In addition, attacks against D-PKGs are identified and anonymizing of D-PKGs is proposed as a countermeasure. Moreover, the experiment determines the optimal secret sharing parameters to achieve maximum security.

El-Khatib *et al*. (2005) studied the possibility of achieving anonymity in ad hoc networks and proposed an anonymous routing protocol, similar to onion routing concept used in wired networks. While data encryption can protect the content exchanged between nodes, routing information may reveal valuable information about end users and their relationships. The proposed protocol includes a mechanism to establish a trust among mobile nodes while avoiding untrustworthy nodes during the route discovery process. The major objective of the protocol is to allow only trustworthy intermediate nodes to participate in the routing protocol without jeopardizing the anonymity of the communicating nodes. The simulation results indicate clearly that anonymity can be achieved in mobile ad hoc networks and the additional overhead of our scheme to DSR is reasonably low when compared to a non secure DSR ad hoc routing protocol.

MATERIALS AND METHODS

The concept of ants looking out for food are used in this work for performing the proactive routing were the agents use ants to periodically gather the routing information between different source-destination pairs to reduce the route discovery latency. Ant colony optimization (ACO) is a population-based metaheuristic used for finding solutions for optimization problems. In ACO, artificial ants search for good solutions in form of finding optimal path in a graph. The search is based on the behavior of ants searching for a path between their colony and a source of food. The ACO finds solution by finding the best path on the weighted graph. The solutions are constructed on the basis of pheromone model and are incrementally built by moving on the graph. The ant builds the solution and evaluates the solution and modifies as required by modifying the trail values of the components used in the solution. The components are either edges or nodes in the graph. This pheromone information is used by future ants.

For applying ACO, the problem is defined as a model with search space of finite set of discrete decision variables, set of constraints among variables and an objective function. The set of feasible solutions is given by elements in the search space satisfying all the constraints.

To construct Ant solutions, a set of m artificial ants from elements of a finite set of available solution components $C = \{cij\}$, $i = 1,\ldots,n$, $j = 1,\ldots,|Di|$. A solution construction starts with an empty partial solution $s^p = \phi$. Then partial solution sp is added in form of feasible solution component from the set of feasible neighbors, at each construction step.

The choice of a solution component from N(sp) is done probabilistically at each construction step. Different ACO variants has different rules for the probabilistic choice of solution components. The best known rule is the one of Ant System (AS) (Dorigo *et al*., 1996):

$$p(c_{ij} \mid s^p) = \frac{\tau_{ij}^{\alpha}\eta_{ij}^{\beta}}{\sum c_{ij} \in N(s^p)\tau_{ij}^{\alpha}\eta_{ij}^{\beta}}, \forall c_{ij} \in N(s^p)$$

where, τ_{ij} and η_{ij} are respectively the pheromone value and the heuristic value associated with the component cij. α and β are positive real parameters giving the relative importance of pheromone versus heuristic information

As more ants move, the particular pheromone entry increases and hence that neighbor gets more probability. The quality of the link life, energy depletion rate of neighbors and processing power of the neighbors affect the probability values of the neighbors. When the request ant passes through various nodes, it collects the information about the trust and reputation. Information about the node is expressed in terms of a normalized index that varies between 0 and 1. The request ant collects the information about the quality of the nodes all along the route and determines the quality of the overall path as a product of the trust and reputation of individual nodes. When the request ant reaches the destination, the destination grades the quality of the path against the reference value it maintains. Based on the grade received through reply ants, the intermediate nodes update the pheromone values. To mimic the behavior of real ant colony, pheromones deposited are reduced with respect to an evaporation factor. The purpose of this evaporation is to enable the nodes to forget the older paths as the topology and scenario of the wireless network changes.

This study proposes to model a novel routing algorithm which addresses trust and anonymity in routing. Many works are proposed in the literature on authentication and encryption mechanisms in routing and data transfer but not on trust and anonymity. The proposed method is based on the cluster head routing, where a leader node is selected based on the trust of the node in the network and the leader acts as the gateway between the source and destination leader. The source leader node encrypts the source ID for all the communications. Whenever a source node wants to send data, the source leader node uses the hash key to rename the source ID. So that the intermediate nodes have no intimation of the source node ID. The RREQ is broadcasted and if the recipient is an intermediate leader or destination leader it decrypts the destination id and checks whether it is present in its local table. Thus, anonymity is achieved between the source and the destination.

The snapshot of the scenario is given in Fig. 1. The architecture of the proposed routing protocol consists of the following message packets:

- Route Request (RREQ)
- Route Reply (RREP)
- Route Error (RERR)
- HELLO for route maintenance

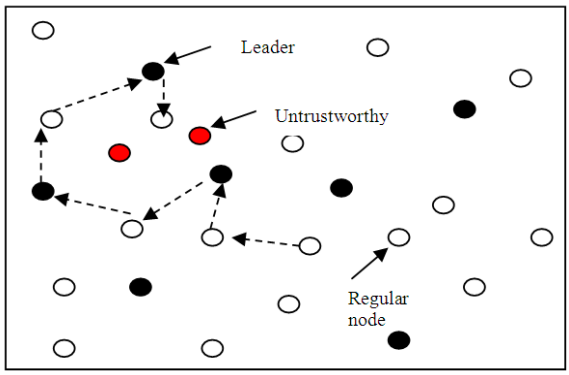

Fig. 1: Snapshot of the network and the route taken

Source leader Id
Hashed destination Id
. . . .
. . . .
. . . .
Low pheromone node

Fig. 2: The RREQ format in the proposed routing protocol

TBLSR format		LSR format
Source Id		Destination Id
Trust value		Source Id
Hop count value		Hop count
Time stamp		Strength of pheromone
Intermediate node Id		Trust value
(a)		(b)

Fig. 3: TBLSR and LSR header format in the proposed protocol

In the proposed protocol, RREP is generated only by the destination node. Intermediate nodes do not reply thus increasing the overall security. The RREQ, RREP and the RERR have the basic AODV packet format with modifications to avoid nodes where trust level is very low. An additional field "Known Low Pheromone Route" (LPN) is included in the AODV format of RREQ packet. It is proposed to add two more message format in addition to the above message format:

- Trust Based Leader Select Request (TBLSR)
- Leader Select Reply (LSR)

The format of the RREQ in the proposed routing protocol is shown in Fig. 2.

The source leader can receive more than one RREP packet to the destination leader. The route is selected

based on the overall pheromone strength in the entire path. The structure of TBLS and LME is shown in Fig. 3a and 3b.

A TBLSR message is generated with current pheromone value and timestamp whenever a source node wants to send data to a destination node. Based on the Hop Count Value (HCV) the intermediate node replies to the source using LSR with its pheromone strength and the number of times it has successfully acted as a leader node. It then decrements the HCV, if HCV ≠ 0 it broadcasts the TBLSR and updates the Intermediate Node Id with its ID. All nodes receiving the TBLSR request reply with LSR. The highest trust value from the received LSR forms the basis of selecting leader node.

The source sends RREQ only to the selected leader node using LPN field to avoid nodes with low trust values. The leader node receives the request and encrypts the source address and sends RREQ. The intermediate forwards the RREQ request and the destination replies by RREP. Thus an anonymous relationship is established between source and destination.

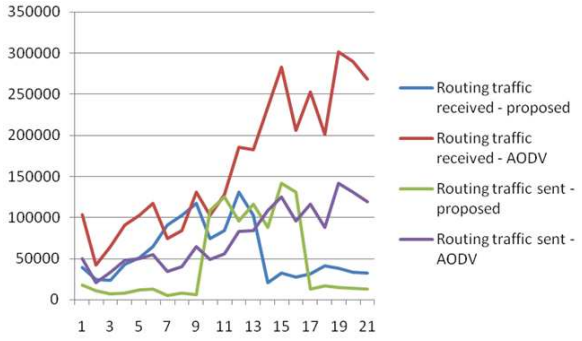

Fig. 4: The control packet overheads for AODV and the proposed protocol

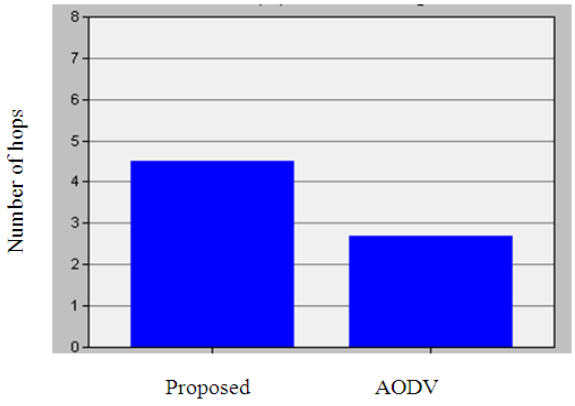

Fig. 5: The average hop count for the proposed routing and AODV

RESULTS

The experimental set up consisted of 26 wireless devices spread over 0.25sq Km. 4 of the nodes were either selfish or malicious nodes with low trust values. Each of the node moves about randomly. Two scenarios were considered with existing AODV routing and proposed routing method. Figure 4 shows the control packet overheads.

The average hop count for both the protocols is shown in Fig. 5.

The control overhead increases as shown in Fig. 4 due to additional control packet overheads from TBLSR and LSR. Similarly the hop count increases in the proposed protocol (Fig. 5) as some of the nodes are not used for routing mentioned in LPN.

DISCUSSION

A novel routing protocol Mobile Anonymity based on Ant Colony Optimization (ACO) was proposed. The proposed routing protocol added two more control packets and modified the RREQ packet of the AODV routing protocol to avoid nodes with low trust factor. The output obtained improves the overall MANET security by eliminating nodes which do not meet the trust criteria.

CONCLUSION

In this study it was proposed to address anonymity and trust for a wireless network containing selfish and malicious nodes. The proposed method increases the control overhead of the network by almost 100% which can be a disadvantage in bandwidth constrained large networks.

REFERENCES

Asokan, R., A.M. Natarajan and A. Nivetha, 2007. A swarm-based distance vector routing to support multiple Quality of Service (QoS) metrics in mobile adhoc networks. J. Comput. Sci., 3: 700-707. DOI: 10.3844/jcssp.2007.700.707

Boukerche, A., K. El-Khatib, L. Xu and L. Korba, 2004. SDAR: A secure distributed anonymous routing protocol for wireless and mobile ad hoc networks. Proceedings of the 29th Annual IEEE International Conference on Local Computer Networks, Nov. 16-18, IEEE Xplore Press, pp: 618-624. DOI: 10.1109/LCN.2004.109

Boukerche, A., K. El-Khatiba, L. Xua and L. Korbab, 2005. An efficient secure distributed anonymous routing protocol for mobile and wireless ad hoc networks. Comput. Commun., 28: 1193-1203. DOI: 10.1016/j.comcom.2004.07.019

Chen, J., R. Boreli and V. Sivaraman, 2010. TARo: Trusted Anonymous Routing for MANETs. Proceedings of the IEEE/IFIP 8th International Conference on Embedded and Ubiquitous Computing (EUC), Dec. 11-13, IEEE Xplore Press, Hong Kong, pp: 756-762. DOI: 10.1109/EUC.2010.119

Dorigo, M., V. Maniezzo and A. Colorni, 1996. Ant system: Optimization by a colony of cooperating agents. IEEE Trans. Syst. Man Cybern. B Cybern., 26: 29-41. PMID: 18263004

El Defrawy, K. and G. Tsudik, 2008. PRISM: Privacy-friendly routing in suspicious MANETs (and VANETs). Proceedings of the IEEE International Conference on Network Protocols, Oct. 19-22, IEEE Xplore Press, Orlando, FL., pp: 258-267. DOI: 10.1109/ICNP.2008.4697044

El-Khatib, K., L. Xu and L. Korba, 2005. A novel solution for achieving anonymity in wireless ad hoc networks. Proceedings of the 1st ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor and Ubiquitous Networks, Oct. 4-6, ACM Press, Venice, Italy, pp: 30-38. DOI: 10.1145/1023756.1023763

Gopalakrishnan, K. and V.R. Uthariaraj, 2011. Acknowledgment based reputation mechanism to mitigate the node misbehavior in mobile ad hoc networks. J. Comput. Sci., 7: 1157-1166. DOI: 10.3844/jcssp.2011.1157.1166

Guan, Y., X. Fu, D. Xuan, P. Shenoy and R. Bettati *et al*., 2001. NetCamo: Camouflaging network traffic for QoS-guaranteed mission critical applications. IEEE Trans. Syst. Man Cybern. A Syst. Hum., 31: 253-265. DOI: 10.1109/3468.935042

Kong, J. and X. Hong, 2003. ANODR: Anonymous on demand routing with untraceable routes for mobile ad-hoc networks. Proceedings of the 4th ACM International Symposium on Mobile Ad Hoc Networking and Computing, Jun. 1-3, ACM Press, Annapolis, MD, USA., pp: 291-302. DOI: 10.1145/778415.778449

Mohapatra, P. and S. Krishnamurthy, 2005. Ad Hoc Networks: Technologies and Protocols. 1st Edn., Springer, New York, ISBN-10: 0387226893, pp: 270.

Nekkanti, R.K. and C.W. Lee, 2004. Trust based adaptive on demand ad hoc routing protocol. Proceedings of the 42nd Annual Southeast Regional Conference, Apr. 2-3, ACM Press, Huntsville, AL, USA, pp: 88-93. DOI: 10.1145/986537.986558

Netrvalova, A. and J. Safarik, 2009. Interpersonal trust model. University of West Bohemia.

Sabari, A. and K. Duraiswamy, 2009. Multiple constraints for ant based multicast routing in mobile ad hoc networks. J. Comput. Sci., 5: 1020-1027. DOI: 10.3844/jcssp.2009.1020.1027

Shao, M.H. and S.J. Huang, 2008. Trust enhanced anonymous routing in mobile ad-hoc networks. Proceedings of the 9th International Conference on Parallel and Distributed Computing, Applications and Technologies, Dec. 1-4, IEEE Xplore Press, Otago, pp: 335-341. DOI: 10.1109/PDCAT.2008.10

Sun, Y. L., Z. Han, W. Yu and K.J.R. Liu, 2006. A trust evaluation framework in distributed networks: Vulnerability analysis and defense against attacks. Proceedings of the 25th IEEE International Conference on Computer Communications, Apr. 23-29, IEEE Xplore Press, Barcelona, pp: 1-13. DOI: 10.1109/INFOCOM.2006.154

Suresh, A. and K. Duraiswamy, 2011. Mobile ad hoc network security for reactive routing protocol with node reputation scheme. J. Comput. Sci., 7: 242-249. DOI: 10.3844/jcssp.2011.242.249

Yang, L., M. Jakobsson and S. Wetzel, 2006. Discount anonymous on demand routing for mobile ad hoc networks. Proceedings of the Securecomm and Workshops, Aug. 28-Sept. 1, IEEE Xplore Press, Baltimore, MD., pp: 1-10. DOI: 10.1109/SECCOMW.2006.359533

Zhang, Y., W. Liu, W. Lou and Y. Fang, 2006. MASK: Anonymous on-demand routing in mobile ad hoc networks. IEEE Trans. Wireless Commun., 5: 2376-2385. DOI: 10.1109/TWC.2006.1687761

Zhang, Y., W. Liu, W. Lou, Y. Fang and Y. Kwon, 2005. AC-PKI: Anonymous and certificateless public-key infrastructure for mobile ad hoc networks. Proceedings of the IEEE International Conference on Communications, May 16-20, IEEE Xplore Press, pp: 3515-3519. DOI: 10.1109/ICC.2005.1495073

Zou, C. and C. Chigan, 2009. An anonymous on-demand source routing in MANETs. Secur. Commun. Netw., 2: 476-491. DOI: 10.1002/sec.79