International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 4 (2015) pp. 10415-10430

http://www.ripublication.com

Mobile Anonymous Trust Routing For Ad Hoc Networks Using Ant Colony Optimization

1Dr. R. KALPANA, 2B. MADHUSUDHANAN

1Professor, Department of CSE, IFET College of Engineering, Villupuram, India
2Asst.Profesor, Department of CSE,
Er.Perumal Manimekalai College of Engineering, Hosur, India
E-mail: kalpana5615@gmail.com

Abstract

In this paper a mechanism to address anonymous routing with trust to improve overall ad hoc network security and performance is proposed. Ad hoc networks are vulnerable to denial of services, wormhole attacks and spoofing. End-to-end data security in a network is generally provided by encryption and authentication which increases the overheads, but node's topology information can be acquired through studying traffic/routing data. Improving the ad hoc network security and its performance using anonymity mechanisms and trust levels is investigated in this paper. Anonymous networks hide identification information such as traffic flow, network topology, paths from malicious attackers. Trust is a prerequisite as selfish/ malicious nodes are a security hazard, decreasing Quality of Service (QoS). Routing based on security mechanisms is proven to be a NP Hard problem. To overcome this, it is proposed to use Ant Colony Optimization (ACO) for faster convergence of the proposed solution. Results show that overall network security improves when the trust factor is taken into account with definite improvement in the QoS.

Keywords: Ad hoc network, Anonymous Networks, Trust and Reputation, Security, Ant Colony Optimization (ACO)

Introduction

Mobile Ad-hoc NETwork (MANET) the latest paradigm of wireless communication; made of collection wireless devices which allows communication with other nodes within its radio range. Nodes are interconnected by wireless links in an ad hoc manner and act as both host and routers [1]. The nodes communicate in single hop or multi-hop paths, and intermediate nodes are routers. Ad hoc networks inherent

dynamic nature, infrastructure-less and the broadcasting nature make it vulnerable to malicious traffic attacks. Neighboring nodes are either friendly or hostile; so information passed through an ad-hoc network route should be protected to ensure security/anonymity of exchanged information [2]. Various studies were undertaken over the years in this regard. Ensuring routing and data packets security for propagation is the foundation of most research. Anonymous routing is an added advantage in maintaining security and privacy. Anonymization has attained popularity recently and is being widely researched. But very few studies relatively address the issue of trust based anonymous routing [3].

Ad hoc routing protocol security is incorporated through techniques like encryption, authentication, anonymity and trust factors. Encryption and authentication ensure the end-to-end security mechanisms for data transfer, but information about nodes location and nature is obtained through studies of traffic and routing data [4]. Ad hoc networks security issues are overcome through using anonymity mechanisms and trust levels.

Traditional routing protocols are based on the naïve trust model, where nodes inherently trust all network nodes. Hence they are susceptible to attacks by a malicious network node which can insert incorrect routing information, route erroneous updates or resend old messages. The protocol's security and robustness are enhanced when trust is included in the framework. Trust is quantified by the use of route trust and node trust metrics [5]. Malicious network nodes are identified and isolated by a trust based framework which also evaluates route dependability. Literature [6, 7] provides general frameworks for a network's trust establishment.

Anonymous networks mask network traffic communication information to increase communication privacy and to repel intrusions/attacks. Identification information paths - similar to traffic flow and network topology - is concealed to all network nodes in an anonymous network. The nodes include both bonafide and malicious nodes [8]. Ad hoc routing protocols aided by anonymity measures protects both node privacy and information flow by the malicious nodes. Attacks like address spoofing, traffic analysis and certain Denial of Service (DoS) attacks are prevented in anonymous network by hiding the traffic's real identity. Many anonymous routing protocols are proposed in the literature [9, 10, 11].

Swarm intelligence (SI) is the total behaviour of a decentralized, self-organized group [12, 13] adapted for designing novel algorithms for distributed optimization and control. SI includes mobile software agents for network management interacting with the environment and amongst themselves. These agents are autonomous, and both proactive and reactive having the capability to adapt, cooperate and move intelligently between locations in a communication network [14]. Agents follow simple rules and have limited capabilities. They do not follow centralized orders for every individual or interact locally/randomly. But together their behaviour is seen as "intelligent". From a global viewpoint, swarms nature resembles MANET and solves routing problems [15]. SI emphasizes a bottom-up design of autonomous distributed systems which are adaptive, robust, and scalable in nature. Ant colony algorithms (ACO) [16, 17] and Particle Swarm Optimization (PSO) [18] are popular SI frameworks.

Ants foraging behavior is used to solve complex problems in ACO. Though solutions are based on ant's cooperation, they do not communicate directly but through stigmergy. Various problems including optimization are overcome successfully through ACO based algorithms [19]. The analogy between such biological systems and network routing is that the ants are looked at as a distributed adaptive system of smart control packets, each of which uses little computational and energy resources to explore its network/environment. They cooperate by releasing information about the discovered paths and their estimated quality at the nodes [20].

This paper combines anonymity and trust factors in routing to improve ad hoc network security without compromising on QOS. Inspite of encryption and authentication providing end-to-end data security, they also increase network overheads which is a disadvantage in ad hoc networks. Anonymity is used as a cover for routing data while trust improves end-to-end security. The proposed routing is an extension of Ad-hoc On-demand Distance Vector (AODV) algorithm with trust and anonymity. The remainder of the paper is structured as follows: Section 2 summarizes related works available in the literature. Materials and proposed methods used in this investigation are discussed in section 3. Section 4 relates both experimental setup and simulation results. Section 5 concludes the paper.

Related Works

Literature has many examples related to anonymous routing. Boukerche et al. (2004) [8] proposed a novel distributed routing protocol to locate secure, reliable and anonymous routes in a hostile environment which encrypts routing packet header, avoiding unreliable intermediate nodes enroute. The proposed protocol's highlights include non-source-based routing, flexible route selection and robustness against path hijacking. Zhang et al. (2005) [21] presented MASK, a novel anonymous on-demand routing protocol, to obtain anonymity in MAC-layer and network-layer communications. Yang et al. (2006) [22] proposed Discount ANODR based on ANODR to solve the issue of an on demand routing protocol at reduced cost. In this protocol, route onions channel the data packets to destinations with intermediaries knowing only the request destination and the previous intermediary's identity.

Zou and Chigan (2009) [23] proposed a novel Anonymous on Demand Source Routing (AODSR) protocol to ensure sender, receiver and sender-receiver relation anonymity in MANETs. Route discovery is initiated by a series of random residual hop numbers and not by initiator/target node in the protocol. Initiator/target node and intermediate nodes behaviour are eliminated, and route packets flooding are prevented. El Defrawy and Tsudik (2008) [10] presented PRISM, to achieve privacy and security against both outsider/insider adversaries., Incorporating privacy using location-centric communication paradigm is feasible in suspicious ad hoc networks as compared to the address based communication. Chen et al. (2010) [9] suggested a novel anonymous routing protocol to provide both improved anonymity and security. In this method anonymity is achieved through the use of invisible implicit addressing based on keyed hash chain. The Diffie-Hellman mechanism exchanges symmetric encryption keys to secure information. Investigations reveal that anonymity is maintained for all route

nodes, i.e., source, destination and the intermediate nodes privacy is secured against internal and external enemies.

Nekkanti and Lee (2004) [24] proposed a routing protocol to safeguard routing information from unauthorized access. Here, the algorithm chiefly uses a node's trust factor with its neighbor. Transmitted data is encrypted at various levels based on the trust factor and the data packet's security level. Netrvalova and Safarik (2008) [7] were into interpersonal trust modeling where the model integrates – for trust determination - various factors affecting trust. Factors like reciprocal trust, initial trust, subject reputation, number of subject recommendations and mutual contacts and trusting disposition are considered. An interpersonal trust model was developed by incorporating trust evolution factors. Shao and Huang (2008) [25] proposed a reliable protocol where communicating parties can select a secure end-to-end route free from untrustworthy nodes during anonymous route discovery. The proposed protocol accomplishes anonymity-related goals, trust-aware anonymous routing, and effective pseudonym management. Trust-aware anonymity solutions discover reliable routes and remove untrustworthy nodes thereby securing data forwarded in addition to maintaining the anonymity.

This study proposes to model a novel routing algorithm by incorporating both trust and anonymity in routing. Routing authentication and encryption mechanisms and data transfer are the foundation for research in literature but not trust and anonymity alone.

Materials and Methods

Ad-hoc On-demand Distance Vector (AODV)

Ad-hoc On-demand Distance Vector (AODV) is a loop-free routing protocol for ad-hoc networks, designed to be a self-starter among mobile nodes and which can withstand varied network behavior like node mobility, link failures and packet losses [26]. This protocol includes two mechanisms, Route Discovery and Route Maintenance. AODV is selected as it is simple with low overhead, and its on-demand nature is easy on networks.

The following fields exist in AODV route table entry:

- Destination IP Address: The destination IP address for which a route is supplied
- Destination Sequence Number: It is associated with the route.
- Next Hop: Either destination or an intermediate node designated to forward packets to the destination
- Hop Count: The hop number from Originator IP Address to Destination IP Address
- Lifetime: Time in milliseconds, where nodes receiving RREP consider it to be valid
- Routing Flags: State of a route; up (valid), down (not valid) or in repair

Trust

Three primary aspects are linked to distributed networks trust evaluation. First, trust

evaluation ability provides good behaviour with incentives. Ensuring anticipation that entities will "remember" good behaviour ensures responsibility in network participants. Secondly, trust evaluation predicts future behaviour and aids decision-making. It ensures good entities avoid working with untrustworthy parties. Malicious users have low trustworthiness, and hence limited ability to interfere in network operations. Thirdly, trust evaluation results directly detect selfish/malicious network entities.

Figure 1 presents the flow chart of the proposed algorithm to establish trust in MANETs. Each node calculates trust for surrounding nodes and stores such values locally for later use. As mentioned earlier, these values, based on new interactions, are updated in a specific time period. The idea of the algorithm given in Figure 1 is about risk value associated with every job processed by a node. This in turn is derived from the trust value needed for a specific task.

The first thing a node does when performing a task is to compare predefined risk value wedded to the task with actual intra-nodal risk. When risk value is less than the predefined threshold, the task is performed, or else it is avoided unless the node is ready to risk it. The algorithm compares risk values and combines direct trust and indirect trust to achieve total trust before finally calculating actual risk. It does not calculate direct or indirect trust as this is done by the node. Only nodes trust assessment is discussed. A detailed illustration of the algorithm follows. A required trust value is given based on the required security. Trust associated with each job is processed by a node and finally trust value reveals the risk value involved. Trust value (T) is tested against trust sources, direct trust value (A), indirect trust value (B), and total trust value (C). Risk value (R) is calculated simultaneously. If a combination of these values is greater than or equal to required trust value, risk value is less than or equals a predefined risk value (threshold), then the job is processed, or else declined. In other words if a node (X) wants to process a job by another node (Y), then node (Y) first checks any earlier experience with node (X) and if so, then is the trust value (A) given in equation (1)

$$A = \sum_{i=1}^{n} T_{y_i} \quad x \tag{1}$$

where, $T_{y_i} \quad x$ trust value of the ith trust category and *n* number of trust categories.

If (A) is greater than or equal to (T), associated risk is less than the risk threshold, then node (Y) will undertake the job for node (X), or else node (Y) will check any recommendations about node (X) from surrounding nodes. If so that trust value (B) as given in equation (2)

$$B = \frac{\sum_{y=1}^{m} T_y \quad x}{m} \tag{2}$$

where $T_y \quad x$ trust value of node Y on Node X and m number of surrounding nodes.

If (B) is greater than or equal to (T) the associated risk is less than risk threshold. Then node (Y) does the job for node (X), otherwise node (Y) will check combined trust value (C) of (A) and (B), as given in equation in equation (3)

$$C = A*W_A + B*W_B \quad (3)$$

where W_A and W_B are weights assigned.

If (C) is greater than or equal to (T) the associated risk is less than risk threshold, then node (Y) will complete the job for node (X), or else declines it unless the node is ready for the risks associated with that job.

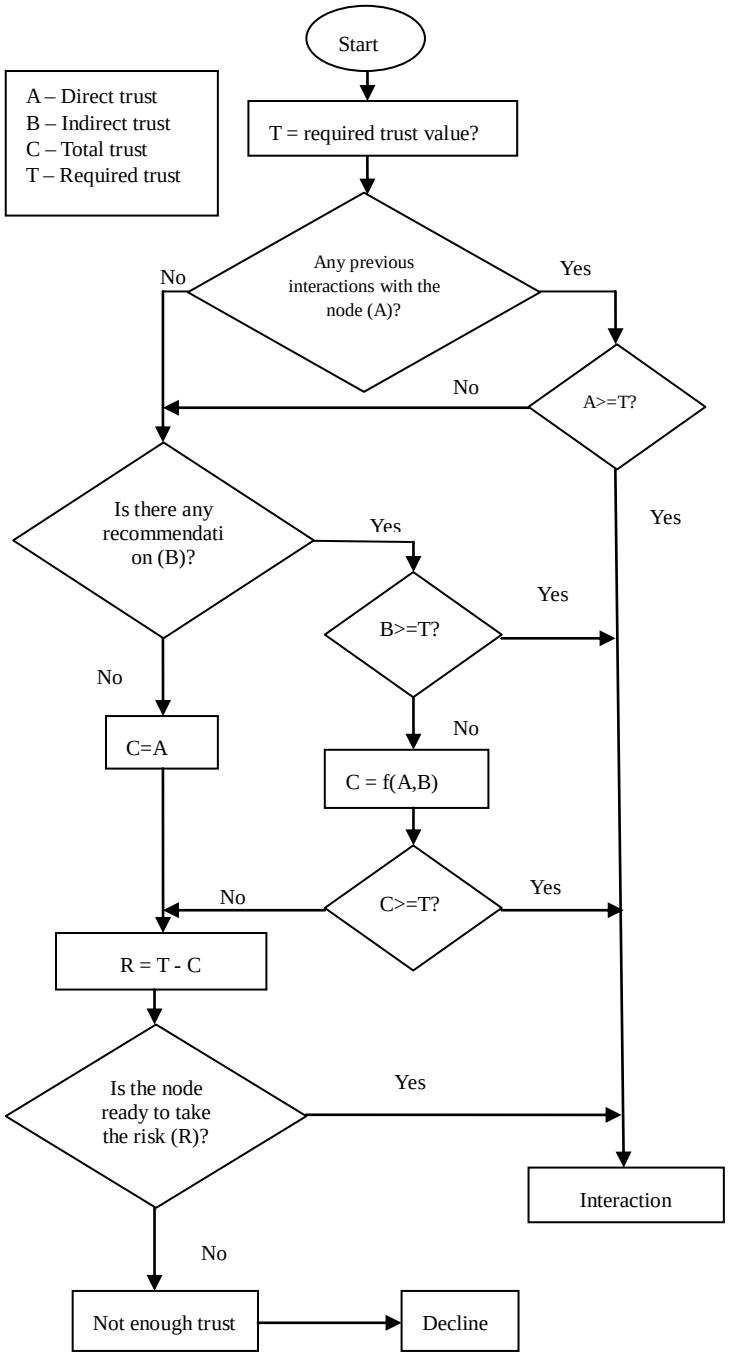

Figure 1: Trust computation Flow chart

Ant colony algorithms (ACO)

Ant colony optimization (ACO) is a population-based metaheuristic used for solving optimization problems. The idea of ants searching for food is used in this work for proactive routing. Agents use ants at regular intervels to get routing information between different source-destination pairs to reduce route discovery latency. It was seen that ants in a colony converge by moving over the shortest among different paths between their nest and food source. [27, 28]. Pheromone a volatile chemical susbstance is the catalyst of this colony-level shortest path behavior; ants moving between nest and food source deposit pheromone, and move toward pheromone concentrated areas. [29]. Shorter paths are completed quicker and visited frequently by ants and hence higher pheromone concentration. These paths attract more ants, which increases pheromone levels, till the majority of ants converge through the shortst path. Pherpomone signals based ants indirect communication and coordination is called stigmergy [31].A novel routing protocol to address anonymous routing with trust which improves the overall security of the ad hoc network [30].

ACO routing algorithms [27] mimic this ant behavior,based on acquisition of routing information by a collective learning process founded on path sampling using ant-like control packets (agents). These agents are generated concurrently/ independently at nodes aimed to try a path to a specific destination. An ant agent (forward ant) moving from source s to destination d collects path quality information (e.g. end-to-end delay and number of hops), and on its way back from d to s (backward ant), uses the information to update routing tables at intermediate nodes. Routing tables, known as pheromone tables, contain a vector of real-valued entries for every destination. The entries in the pheromone tables - the pheromone variables - measure the goodness of going through that neighbor when returning to the destination. This is constantly updated according to path quality sampled by ants. Repeated/concurrent ant agents lead to multiple path availability for each node.

The problem is defined as a model with search space of a finite set of discrete decision variables, set of constraints among variables and an objective function to apply ACO. A feasible solutions set is provided by elements in the search space that satisfies all constraints.To construct Ant solutions, a set of m artificial ants from elements of a finite set of available solution components $C = \{c_{ij}\}$, $i = 1,\ldots,n$, $j = 1,\ldots,|Di|$. A solution construction begins with an empty partial solution $s^p = \phi$. Then partial solution s^p is added in the form of a feasible solution component from feasible neighbors set at each construction step.

The choice of a solution component from $N(s^p)$ is done probabilistically at each construction step. Different ACO variants have different rules for probabilistic choice of solution components. The best known rule is the Ant System (AS) [32] is shown in equation (4)

$$p(c_{ij} \mid s^p) = \frac{\tau_i^{\alpha} \eta^{\beta}{}_{i\,j}}{\sum c_{ij} \in N(s^p) \tau_{ij}^{\alpha} \eta_{ij}^{\beta}}, \forall c_{ij} \in N(s^p) \tag{4}$$

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

Proposed Methodology - Mobile Anonymous Trust Routing (MACT)

In the proposed Mobile Anonymous Trust Routing (MACT), as more ants move pheromone entry increases and so that neighbor gets more probability. Link life quality, neioghbours energy depletion rate and processing their power affect their probability values. The request ant passings through various nodes, collects trust and reputation information. Node information is expressed in terms of a normalized index ranging between 0 and 1. The request ant collects information about node quality along the route and determines overall path quality as a trust product and iondividual nodes reputation. The destination grades path quality after the request ant reaches it against the maintained reference value. Based on reply ants grade, intermediate nodes update pheromone values. Deposited pheromones are reduced with respect to an evaporation factor to mimic real ant behaviour. Evaporation enables nodes to forget older paths when wireless network scenario and topology change. Ant Optimization steps used in the Proposed Routing is revealed in Figure 2.

Based on the network node trust, a leader node is selected as a gateway between source and destination leader. The source leader node encrypts all communication for source ID. When a source node plans to forward data the hash key renames the source ID, thereby masking it form intermediate nodes. RREQ is broadcast during route recovery and intermediate/destination leader on receipt of RREQ decrypts it to see destination id and checks the presence in the local table, thereby ensuring anonymity between source and destination.

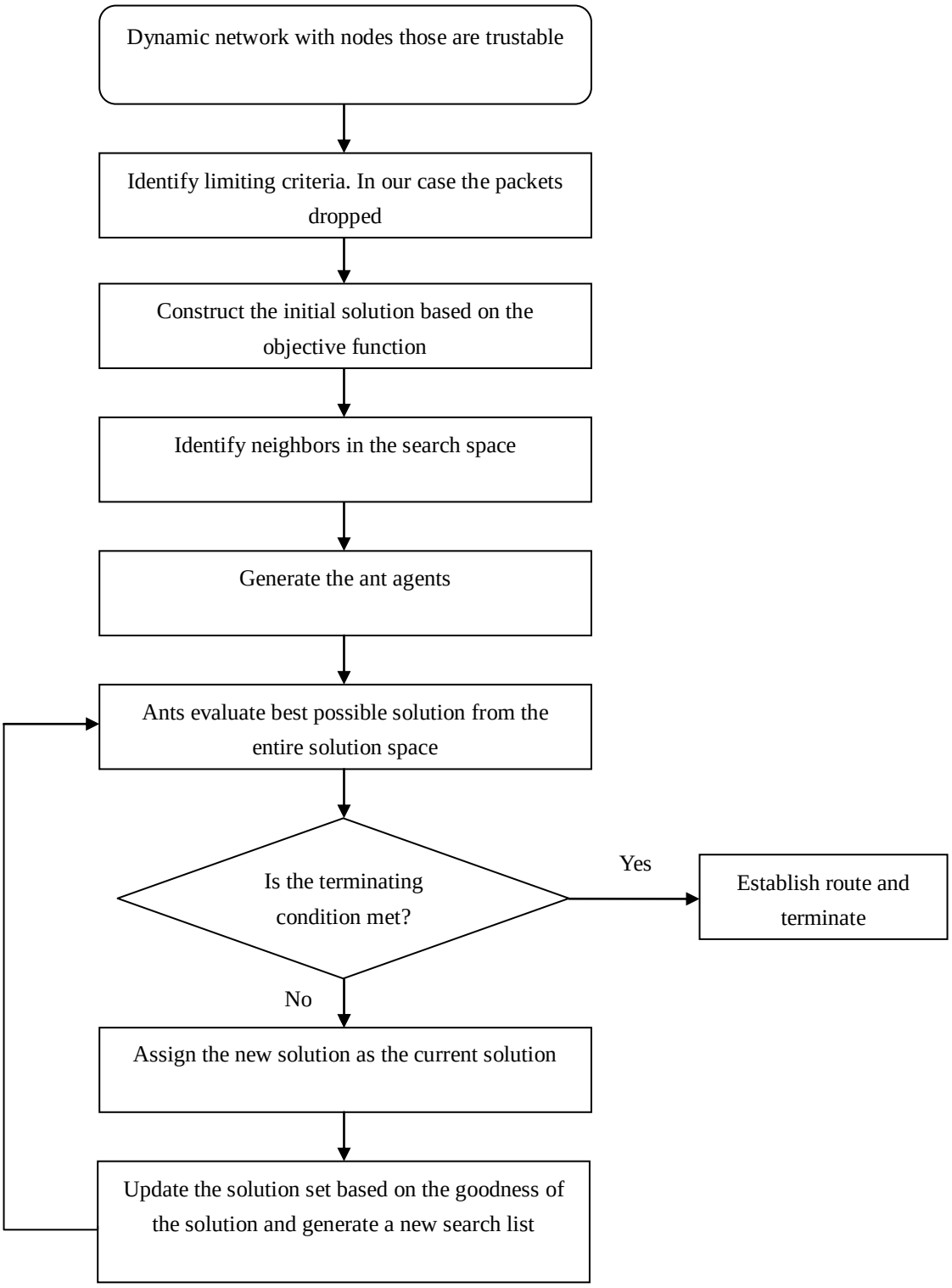

Figure 2: Flow Chart of Ant Optimization used in the Proposed Routing

The snapshot of the scenario is given in Figure 3. 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

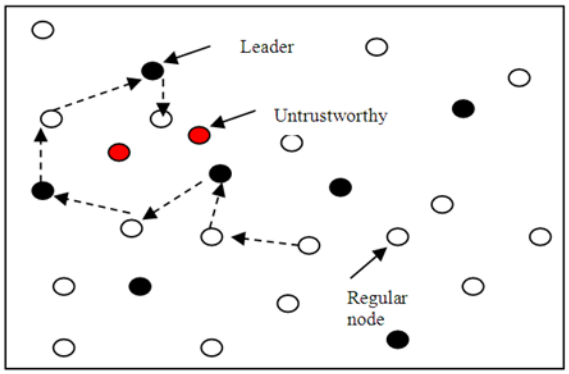

Figure 3: Network Snapshot and the Route taken

Only destination nodes generate RREP in the propsoed protocol.Overall security is increased as intermediate nodes do not reply. RREQ, RREP and RERR have basic AODV packet format with modifications to avoid nodes whose trust level is low. AODV format of RREQ packet includes an additional field "Low Pheromone Node" (LPN). It is proposed to add two additional 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 Figure 4.

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

Figure 4: The RREQ format

Source leader can receive more than one RREP packet to destination leader. Route selection is based on the path's overall pheromone strength. TBLSR and LSR structure is seen in Figure 5a and 5b.

TBLSR format
Source Id
Trust value
Hop count value
Time stamp
Intermediate node Id

(a)

LSR format
Destination Id
Source Id
Hop count
Strength of pheromone
Trust value

(b)

Figure 5: TBLSR and LSR header format in the proposed protocol

When a source node wants to send data to a destination node a TBLSR message is generated with current pheromone value and timestamp. Based on Hop Count Value (HCV) intermediate node replies to the source using LSR with its pheromone strength and the many times it was a sucessful leader node. The HCV is then decremented, HCV ≠ 0 it broadcasts the TBLSR and updates Intermediate Node ID with its ID. All nodes on receipt of TBLSR request reply with LSR. LSR's highest trust value is the basis on which the leader node is selected.

The source sends RREQ only to selected leader node through a LPN field to avoid low trust value nodes. Leader node receives the request, encrypts source address and sends RREQ. The intermediate node forwards RREQ with the destination replyhing by RREP. This establishes an anonymous relationship between source and destination.

The experimental set up consists of 20 to 50 nodes with a varying malicious node percentage. Selfish or malicious nodes have low trust values. Each node moves randomly. Two scenarios were considered with the current AODV routing and proposed optimized Mobile Anonymous Trust Routing (MACT) routing procedures. A 300 sec simulation was carried out.

Results

Simulations are conducted to study packet delivery ratio for 0%, 10%, 20%, 30%, 40%, 50% presence of malicious nodes for differing numbers of network nodes. This (ranging from 20 to 50) is seen in Figure 6-9 with Table 1 tabulating it.

Figure 6-9 reveals that when malicious node percentage escalates from 0 to 50%, network packet delivery ratio decreases drastically. But the same ratio is increased by 3%. Through the proposed optimization, when compared to MACT routing protocol in networks of 30 nodes or less, performance is improved in comparison with the classic AODV. Hence, optimization performs better for smaller networks of 30 nodes or less.

Table 1: Packet delivery ratio for different sized Networks

Percentage of malicious node	Number of nodes =20			Number of nodes=30		
	AODV	MACT	MACT with ACO	AODV	MACT	MACT with ACO
0	0.9823	0.9821	0.9824	0.9812	0.9817	0.9817
10	0.7321	0.8990188	0.92509	0.7127	0.866643	0.883976
20	0.5492	0.681008	0.700076	0.4932	0.608609	0.631127
30	0.4412	0.558118	0.574303	0.4147	0.515057	0.532054
40	0.3756	0.4646172	0.474839	0.3562	0.432427	0.441075
50	0.2184	0.26754	0.272088	0.1987	0.244401	0.248556

Percentage of malicious	Number of nodes=40			Number of nodes=50		
	AODV	MACT	MACT with ACO	AODV	MACT	MACT with ACO
0	0.9806	0.9813	0.9817	0.9801	0.9796	0.9798
10	0.6912	0.8342784	0.86765	0.6314	0.755154	0.790647
20	0.4724	0.5659352	0.592534	0.4287	0.510667	0.531758
30	0.3915	0.462753	0.482189	0.3478	0.408387	0.423554
40	0.3221	0.3794338	0.391955	0.2846	0.329567	0.339783
50	0.1762	0.2065064	0.212082	0.1411	0.165369	0.169834

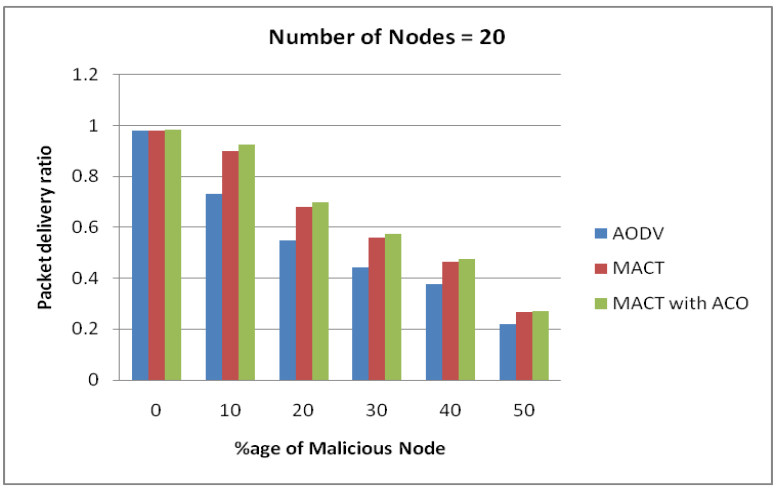

Figure 6: Packet delivery ratio for a network with 20 nodes

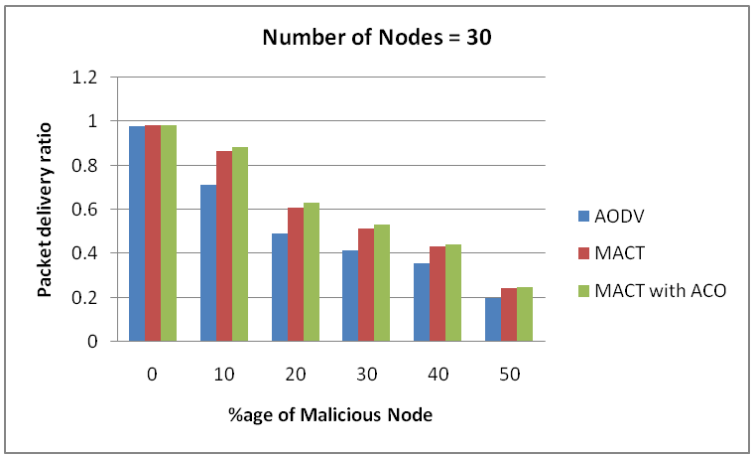

Figure 7: Packet delivery ratio for a network with 30 nodes

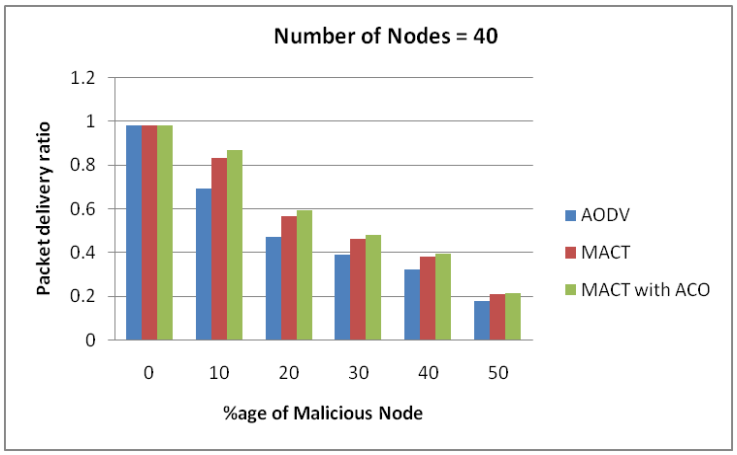

Figure 8: Packet delivery ratio for a network with 40 nodes

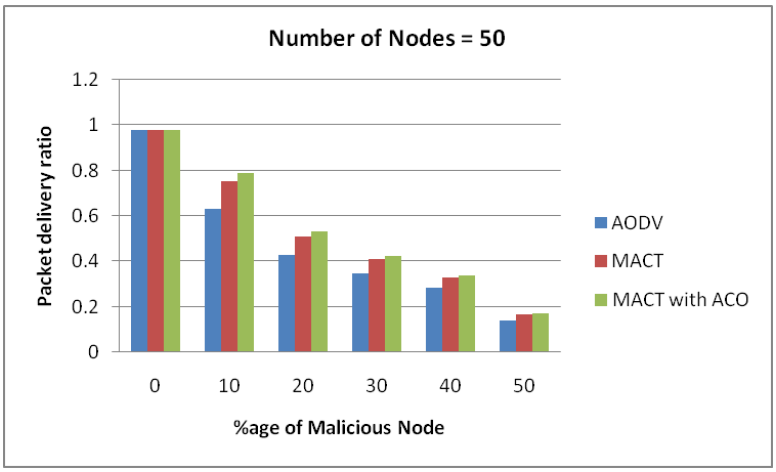

Figure 9: Packet delivery ratio for a network with 50 nodes

From Figures 6-9, it is seen that when the percentage of malicious nodes increase from 0 to 50%, the packet delivery ratio decreases drastically in the network. But, the proposed optimization improves packet delivery ratio by at least 3% when compared to the proposed MACT routing protocol in networks consisting of 30 nodes or less. The performance is much better when compared to classic AODV. The proposed optimization performs better for smaller networks with less than 30 nodes.

Conclusion

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.

In this study, it was proposed to address anonymity and trust for a wireless network containing selfish and malicious nodes. Simulation results show that the packet delivery ratio is considerably in the proposed optimization protocol. The proposed method increases the control overhead of the network by almost 100% which can be a disadvantage in bandwidth constrained large networks.

References

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

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

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

[4] 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 ad hoc networks. J. Comput. Sci., 3: 700-707. DOI: 10.3844/jcssp.2007.700.707

[5] 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

[6] 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. University of Rhode Island, Kingston. http://sig.umd.edu/publications/Sun_INFOCOM_200604.pdf

[7] Netrvalova A., and Safarik J., (2009). "Interpersonal Trust Model." In Proceedings of 6th Vienna International Conference on Mathematical Modelling (Vienna, Austria), pp. 530-537.

[8] 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

[9] 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

[10] 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

[11] 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, Annapolis, MD, USA., pp: 291-302. DOI: 10.1145/778415.778449

[12] Kennedy, J., Eberhart, R.C., Shi, Y., (2001). Swarm Intelligence, Morgan Kaufman, San Francisco, USA.

[13] Engelbrecht, (2007) Computational Intelligence: An Introduction, second ed., Wiley.

[14] Kassabalidis, I., El-Sharkawi, M. A., Marks, R. J., Arabshahi, P., & Gray, A. A. (2001). Swarm intelligence for routing in communication networks. In Global Telecommunications Conference, 2001. GLOBECOM'01. IEEE (Vol. 6, pp. 3613-3617). IEEE.

[15] Stojmenovic, M. (2005). Swarm Intelligence for Routing in Ad Hoc Wireless Networks. Security and Routing in Wireless Networks, Nova Science Publishers, 167-188.

[16] Di Caro, G. A. Ant Colony Optimization and Its Application to Adaptive Routing in Telecommunication Networks, (2004) Ph.D. Thesis, Faculté des Sciences Appliquées, Université Libre de Bruxelles (ULB), Brussels, Belgium.

[17] Di Caro, G. A. Ducatelle, F., Gambardella, L., (2008), Theory and practice of Ant Colony Optimization for routing in dynamic telecommunications networks, in: N. Sala, F. Orsucci (Eds.), Reflecting Interfaces: The Complex Coevolution of Information Technology Ecosystems, Idea Group, Hershey, PA, USA, pp. 11–32.

[18] Bergh, F.V.D., Engelbrecht, A., (2006) A study of particle swarm optimization particle trajectories, Information Sciences 176 (8) 937–971.

[19] Dorigo.M, V. Maniezzo and A. Colorni, (1996). Optimization by a colony of cooperating agents, IEEE Transactions on Systems, Man, and Cybernetics-Part B, 26(1):29-41.

[20] Saleem, M., Di Caro, G. A., & Farooq, M. (2011). Swarm intelligence based routing protocol for wireless sensor networks: Survey and future directions Information Sciences, 181(20), 4597-4624.

[21] 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

[22] 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.

[23] 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

[24] 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

[25] 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

[26] Perkins, C., & Belding-Royer, E. (2003). S. Das," Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, July.

[27] Dorigo, M., Di Caro, G.. A. Gambardella, L. (1999). Ant algorithms for discrete optimization, Artificial Life 5 (2) 137–172.

[28] Goss, S., Aron, S., Deneubourg, J. L., Pasteels, J. M., (1989). Self-organized shortcuts in the Argentine ant, Naturwissenschaften 76 579–581.

[29] Ghosh, A., Halder, A., Kothari, M., Ghosh, S. (2008), Aggregation pheromone density based data clustering, Information Sciences 178 (13) 2816–2831.

[30] Kalpana R & Rengarajan N (2011), MACT – Mobile Anonymous Continuous Trust Based Routing Protocol, European Journal of Scientific Research, Vol.66 No.2, pp. 187-194.

[31] Bonabeau, E., Dorigo, M., Theraulaz, G. (1999) Swarm Intelligence: From Natural to Artificial Systems, Oxford University Press, New York, USA.

[32] Dorigo, M., Maniezzo, V., & Colorni, A. (1996). Ant system: optimization by a colony of cooperating agents. Systems, Man, and Cybernetics, Part B: Cybernetics, IEEE Transactions on, 26(1), 29-41.