Asian Journal of Information Technology 12 (3): 83-90, 2013
ISSN: 1682-3915

Secured Ant Colony Optimization Routing for Wireless Network

[1]D. Srinath and [2]J. Janet
[1]St. Peters University, Chennai, India
[2]Department of CSE, Dr. MGR University, Chennai, India

Abstract: Wireless network becomes unavoidable in the modern world. Routing is a major research area in every communication system which includes multi-hop wireless networks. Attacks which may be passive attacks or active attacks on routing service will collapse the entire operation of the whole network. The attacks on routing services in wireless network are simpler than traditional routing services in the wired networks. Hence, designing a secured a routing attracts many researchers. However, designing such secure routing protocol is not a straightforward procedure. In this study, a secured ant colony optimization is proposed. The ant colony optimization is a swarm intelligence based real time routing protocol which offers highly reliable and optimal routing for both single path and multi path routing. Hence, securing ant colony optimization for wireless network will lead to appreciable result.

Key words: Wireless network, secured routing, ant colony optimization, routing attacks, India

INTRODUCTION

Low deployment cost and more flexible network access are the major causes of rapid spread of wireless networks than the traditional wired networks. These key advantages are leads to deploying wireless networks for many applications where the deployment of wired network is impractical due to the high deployment costs for example, wireless sensor network in defence applications. Depending upon the node capabilities of each wireless node and the required networking infrastructure wireless network has two kinds of architectures, wireless ad hoc network and infrastructure networks. The infrastructure network is a centralized network where a base station will receive and send data to the mobile nodes for example, cellular communication. The ad hoc network is a collection of wireless nodes which self-configuring a network without any centralized infrastructure.

Wireless routing protocols have two main functions to discover routes between the source and the destination node (s) to forward data messages on the discovered routes. In few wireless routing protocols, the second function of routingonly evaluated, for example in location-based routing protocols, the discovery function is reduced to neighbour discovery instead of route discovery.

Route request: A source node S initiates the route discovery to destination D by flooding the network with a route request message: (S→D (RREQ, rnd, S,D, addrS, label In S→S). Where RREQ is route request, rndis a randomly generated request id, label In S→S is the incoming label of S towards S and addrSis the locally unique network address (e.g., MAC address) of S. In fact, label In S→S is a memory address inside the routing table of S and contains an application identifier which originally initiated the route discovery process.

A node J receiving this broadcast message checks whether it has received the request earlier based on rnd, S and D. If so, J silently drops the request. Otherwise, J stores the quadruple (addrS, label In S→S, rnd, lifetime) in its routing table where lifetime is set to a predefined value MaxLifetime and addrSis the local network address of the neighbouring node from which the request is received. The value of lifetime is periodically decremented when the routing table entry is not used. If it reaches the value of zero then the entry is purged from the routing table. At the same time each time the entry is used, the value of lifetime is reset to MaxLifetime. After every node in the wireless network are flooded the route request which received from S each node that received the request has an entry set towards S. In this way, the backward traffic flow is constructed which is defined by the set of all routing entries created at intermediate nodes. This traffic flow is associated with S at the endpoint D.

Route reply: When destination D receives the first request message for instance from node Z, it creates a routing entry similar to all nodes who receive the request. After that D sends a reply to S:D→Z: (RREP, rnd, addrD,

Corresponding Author: D. Srinath, St. Peters University, Chennai, India

labelOutZ→S, label In D→D). Where, RREP is route reply, rndis the random identifier of the corresponding request originated from S, labelOutZ→S is the incoming label of Z towards S (i.e., the outgoing label of D towards S) received in the request and label In D→D is the incoming label of D.

Here, label in D→D is a memory address inside the routing table of D and similarly to S, contains an application identifier which originally initiated the route discovery process. Note that Z is addressed by its incoming label and its local network address which is included in the message header and not listed in the message content. When Z receives the reply, it first creates a routing entry set towards D. This entry contains addrD, rnd and label In D→D where addrDis the local network address of the neighbouring node from which the reply is received. From now on Z can forward messages to D.

Then, Z looks up the entry addressed by labelOutZ→S in its memory (routing table) and forwards the message to the node contained by this entry. All subsequent nodes receiving the reply do the same operations that Z did. In this way, the forward traffic flow is constructed which is defined by the set of all routing entries created at intermediate nodes. This traffic flow is associated with S at the endpoint D. Finally, after S receives the reply, it can send data messages to D.

Route discovery: Intermediate nodes receiving a control message can forward messages between the source/destination nodes but they cannot send messages to them or any other nodes using the same traffic flow. In order to create a separate traffic flow between an intermediate node and an endpoint, the intermediate node must initiate a new route discovery by sending a request message towards the endpoint. Note that this request does not need to be broadcast as the existing traffic flow between the source/destination pair can be used to forward the new request towards the intended endpoint. In order to indicate the proper actions to be taken to the intermediate nodes this type of request is distinguished from the ordinary request message by its message type identifier in the packet header.

Data forwarding: Each node receiving a data packet can determine the next hop by looking up the routing entry addressed by the incoming label retrieved from the packet. Then, the node can update the incoming label in the packet with the outgoing label found in the routing entry. Note that intermediate nodes between endpoints S and D do not need to be aware of identities S and D. All data packets sent between S and D contain the incoming label of the next node on the route and do not need to include further network addresses besides the address of the next node.

Overview of secured routing: For most of the wireless applications required multi-hop routing. As the multi hop routing protocol is carried out on many mobile nodes, the security becomes critical issue in the multi-hop wireless routing protocol. Due to unsecured routing protocol, a misrouted data packets, passive attacks and active attacks on routing packets are normally happened. For example, the injection of a few forged routing messages or the modification of some existing routing messages will leads to devastating effects on the routing performance.

Literature review: Several secure routing protocols have been proposed for ad hoc networks. However, most of these proposals come with an informal security analysis with all the pitfalls of informal security arguments. Although, there are a few exceptions where some attempts are made to use formal methods for the verification of wireless network routing protocols. The protocol is secure if this security objective function results in a non-acceptable value only with a negligible probability where the definition of what is acceptable or not is protocol dependant. This function may be different for different types of routing protocols but the general approach of comparing the output of this function in the dynamic model to a pre-defined acceptable value remains the same. Hence, the study continues varies routing protocols offered till date and its security functions.

Wireless network routing protocols can be classified as proactive, reactive and hybrid routing protocol based on how routing information is retrieved during the route discovery and maintained by network nodes.

Proactive protocols: All nodes continuously monitor links between nodes and they attempt to maintain a consistent, up to date routing information. In order to monitor topology changes, nodes proactively update network state and maintain a route regardless of whether data traffic exists or not. Thus, the overhead of maintaining up to date topology information is usually high. On the other hand, a source can calculate a path to a particular node faster than reactive protocols that is an advantage of these protocols. WRP (Murthy and Garcia-Luna-Aceves, 1996), DSDV (Perkins and Bhagwat, 1994), DREAM (Arnold *et al*., 1998) or OLSR (Jacquet *et al*., 2001) are few example for proactive routing protocol.

Reactive protocols: These protocols are also called on-demand protocols as a routing path is discovered only when it is needed. The route discovery procedure terminates either when a route has been found or when no route is available after the examination of all or some route permutations. As active routes may be disconnected due to node mobility, a route maintenance procedure is always provided to recover from route break-ups. Compared to proactive routing protocols, the control overhead is lower and thus reactive routing protocols have better scalability than proactive routing protocols in wireless networks. However, when using reactive routing protocols, source nodes may suffer from long delays for route discovery before they can forward data packets. DSR (Johnson and Maltz, 1996), AODV (Perkins and Royer, 1999) or TinyLUNAR (Osipov, 2007) are few examples for reactive routing protocols.

Hybrid protocols: These protocols are proposed to combine the merits of both proactive and reactive routing protocols and overcome their shortcomings. In general, hybrid routing protocols for mobile ad hoc networks exploit hierarchical network architectures. Proper proactive and reactive routing approaches are used at different hierarchical levels, respectively. Hybrid routing protocols for mobile ad hoc networks include the ZRP (Pearlman, 1998), ZHLS (Joa-Ng and Lu, 1999) or HARP (Nikaein *et al*., 2000) protocols.

Based on the different objectives and application environments of wireless networks, the routing protocols for wireless network are further classified in following different ways.

Topology-based routing protocols: These protocols typically build a routing topology during the route discovery process that is used later for data forwarding towards the base station.

Topology-based protocols can be hierarchical (e.g., Low Energy Adaptive Clustering Hierarchy (LEACH) (Heinzelman *et al*., 2000), Threshold sensitive Energy Efficient sensor Network protocol (TEEN) (Manjeshwar and Agrawal, 2001), Adaptive Periodic Threshold sensitive Energy Efficient sensor Network protocol (APTEEN) (Manjeshwar and Agrawal, 2002), Zone Routing Protocol (ZRP), Zone based Hierarchical Link State routing (ZHLS) (Joa-Ng and Lu, 1999), Hybrid Ad hoc Routing Protocol (HARP).

Topology-based protocols can be based on distance vector (e.g., TinyOS beaconing, TinyLUNAR (Osipov, 2007), Wireless Routing Protocol (WRP) (Murthy and Garcia-Luna-Aceves, 1996), Destination Sequence Distance Vector Routing protocol (DSDV) (Perkins and Bhagwat, 1994), DSR (Johnson and Maltz, 1996) and AODV (Perkins and Royer, 1999). Topology-based protocols can be based on link-state protocols, for example, Optimized Link State Routing (OLSR) (Jacquet *et al*., 2001). Topology-based protocols can be based on data-centric such as directed diffusion.

Location-based routing protocols: These protocols such as Greedy Perimeter Stateless Routing (GPSR), Greedy Other Adaptive Face Routing (GOAFR), Distance Routing Effect Algorithm for Mobility (DREAM) are also called position-based or geographic routing protocols. Here, each node forwards a packet based on the location of the destination which is carried by the packet and the locations of the forwarding node's neighbours. These protocols are often considered stateless because the nodes do not need to store any additional routing information besides the locations of their neighbours. As a consequence, location-based routing protocols are mainly concerned with the message forwarding function of routing and the discovery function is reduced to neighbour discovery instead of route discovery.

Hybrid protocols: Hybrid protocols use both geographic and topological information to forward data packets (i.e., sensor nodes maintain some additional routing information besides the locations of their neighbours). These protocols are typically designed to incorporate energy-awareness in the simple forwarding process of geographic routing approaches such as Geographic Energy Aware Routing (GEAR) and Energy Aware Routing (EAR).

Survey on secured routing: There are two honest nodes X and Y and node X intends to send a message m to node Y. A1 and A2 are adversarial nodes where A2 is able to interfere with Y's communication but not with X's and A1's communication. Let A1 be in the communication range of X and Y whereas A2 can only communicate with Y. When X transmits m to Y, node A1 overhears m, meanwhile A2 performs jamming to cause Y not to be able to receive m. In order to take this action, A1 and A2 are connected by an out of band channel thus A1 can send a signal to A2 when A2 should start jamming Y's communication. It is also feasible that A2 performs constant jamming for a certain amount of time; afterwards, A1 can send the modified message m' to Y.

The earlier simplest attack methods are composed of the basic message manipulation techniques. These

include dropping, modification, delaying, injection and re-ordering of routing control messages. In both the route discovery and data forwarding processes, the adversary can inject extra packets in order to decrease the throughput of the network and to consume valuable network resources in wireless sensor networks (leading to denial-of-service). In the route discovery phase, injecting a forged control packet can result in corrupt routing states at honest nodes that may ultimately yield increased traffic control as well as shortened network lifetime and increased network delay.

In a Sybil attack, a single adversarial node illegitimately uses multiple identities during the routing process. This can have devastating effects on multipath routing protocols because a node may believe that it routes packets via node disjoint paths while in reality these paths may all go through the adversarial node implementing the Sybil attack. Sybil attacks employed together with tunnelling or wormhole attacks can be even more powerful as the tunnels and the wormholes can be used by the adversarial nodes to share their invented identities.

The node replication attack is the dual of the Sybil attack where the adversary uses the same identity for multiple devices and thus a single adversarial node may be virtually represented in multiple locations in the network. Replication attacks can also severely influence the operation of most routing protocols in the worst case, the adversary can copy the identity of the base station and use it in different locations of the network. If the adversary manages to impersonate the base station then it may be able to attract all traffic to it this is often referred to as the sinkhole attack. All these basic attack methods listed so far can serve as building blocks for further more complex attacks such as the HELLO flood attack against TinyOS beaconing, the creation of routing loops, black and grayhole attacks or route diversion attacks.

MATERIALS AND METHODS

Proposed secured ant colony optimization wireless routing: The detailed survey on ACO in many engineering applications and recent developments in ACO are available by Mohan and Baskaran (2011a, 2012). The ants move in the network randomly at regular intervals to scan the characteristics of large number of network nodes. While moving, they collect information about the network and deliver it to the network nodes. They deliver more updated information about the network at regular interval to the every node in the network (or subnet) which speeds up the optimization process. Every node in the network can function as a source node, destination node and/or intermediate node. Every node has a routing table and the four data structures. The routing table is established in the route discovery phase and updated in the route maintenance phase based on the proposed priority and compound probability rule which uses the four data structures.

Every source node in the network in a regular interval (Δt), generates Forward Ants (FA) and the FA is circulated in the network for searching the destination. Destinations are locally selected according to the data traffic patterns generated by the local workload. Both intermediate and source nodes forward the FA in the same way. The FA carries the path source address, the destination address, the intermediate node identification and the path information. The FA generation rate can be a function of network dynamics, data rate, time, etc. The FA moves in the network searching for the destination using the probability routing table of intermediate nodes. The selection of the next neighbour is done randomly according to the probability distribution function. In the intermediate node, a greedy stochastic policy is applied for choosing the next hop to move. This policy is used for:

- Node-local artificial pheromones
- Node-local problem dependent heuristic information
- Ants memory

While moving, the FA collects the information about the time length/trip time, the congestion status and the node identifier of the intermediate nodes. A sufficient number of the ants visit the neighbour corresponding to the highest probability in the routing table. However, a number of the FA have a probability to visit other nodes and other paths still have a probability to be visited. This will increase the number of the FA visiting nodes in the region around the best path. In addition, it allows a fair number of FA to visit other regions in the network. Unlike flooding, a FA will be forwarded to only one neighbour.

When a FA reaches its destination, the information carried by this FA path will be graded. Then, the FA will be killed and a Backward Ant (BA) will be generated in the destination. The BA carries its corresponding FA's path grade and path's intermediate nodes ID ant it will be send back to the source node by following the reverse path of its corresponding FA. As the BA moves in the reverse path, the intermediate nodes modify their four data structures based on the path grade carried by the BA and accordingly update their probability routing tables.

Finally, the source node receives the BA, updates its tables and kills the BA. FA shares the same queues as data packets so that they experience the same traffic load.

The BA takes the same path as the concern FA travelled but in opposite direction. BA do not share the same link queues as data packets (like FA) they use the higher-priority queues reserved for routing packets since, the only task of BA is to quickly propagate to the pheromone matrices (the information accumulated by the FA).

At regular intervals, Δt from every network node S, forward ant, $F_{s\to d}$ is launched toward a destination node d to discover a feasible, low-cost path to that node and to investigate the load status of the network along the path. The FA shares the same queues as data packets so that, they experience the same traffic load. Destinations are locally selected according to the data traffic patterns generated by the local workload. If f_{sd} is a measure in bits or in the number of packets of the data flow from the source S to the destination d (s→d) then the probability of creating a FA is:

$$p_{sd} = \frac{f_{sd}}{\sum_{i=1}^{n} f_{si}} \quad (1)$$

Ants adapt their exploration activity in this way to the varying data traffic distribution. While travelling towards their destination nodes, the FA keep memory of their paths and of the traffic conditions found. The identifier of every visited node i and the time elapsed since the launching time to arrive at this ith node are stored in a memory stack $S_{s\to d}(i)$. Further the ant builds a path by performing the following steps.

At each source node i each FA headed toward the destination node d by selecting the intermediate node j, choosing among its neighbour which is not visited already. The neighbours j is selected with a probability P_{ijd} computed as the normalised sum of the pheromone τ_{ijd} with a heuristic value η_{ij} taking into account the state (the length) of the jth link queue of the current node I is:

$$p_{ijd} = \frac{\tau_{ijd} + \alpha \bullet \eta_{ij}}{1+\alpha(|N_i|-1)} \quad (2)$$

The heuristic value η_{ij} is a normalised value function (0, 1) of the length of the queue q_{ij} between the node i and its neighbour j is:

$$\eta_{ij} = 1 - \frac{q_{ij}}{\sum_{l=1}^{N} q_{il}} \quad (3)$$

The value of α determines the importance of the heuristic value with respect to the pheromone values stored in the pheromone matrix (τ). The value η_{ij} reflects the instantaneous state of the node's queues and assuming that the queue's consuming process is almost stationary or slowly varying, η_{ij} gives a quantitative measure associated with the queue waiting time. The pheromone values on the other hand are the outcome of a continual learning process. This learning process will register both the current and the past status of the whole network. The two components of the ant decision system, τ and η used for the decision system will act both the combination of long-term learning process and an instantaneous heuristic prediction.

If an ant returns to an already visited node, the cycle's nodes are remove and all the memory about them are deleted. This process helps the system to avoid the count-to-infinity problems.

When the destination node d is reached, the FA $F_{s\to d}$ generates another ant called the backward ant $B_{d\to s}$ and transferred the information stored in the memory of FA then the FA is to be deleted. The FA is deleted if its life time becomes greater than a value of max_life before it reaches the destination node which is similar to TTL (Time to Live) in the TCP.

The flow of FA and BA have some distinctions. The BA takes the same path as the concern FA travelled but in the opposite direction. The FA share the same link queues as data packets but the BA do not share the same link queues as data packets, instead BA uses the higher-priority queues reserved for routing packets. Because the task of BA is to quickly propagate to the pheromone matrices (Fig. 1).

Each time the BA reaches a node i, the trip time of the BA is to be verified that either the present trip time does not exceed the max allowable trip time or lesser than the existing trip time then the number of BA visiting now to the node i is to be added to the pheromone matrix of the concern path. If the BA's trip time is more than the max allowable trip time or it exceeds the available trip time then the information is not to be added.

The pheromone matrix is updated by incrementing the pheromone τ_{ifd} and decrementing the other pheromones τ_{ijd} where i represents the node ID, d is the destination node, f is the current neighbour and j is the existing neighbour where, $j \in N$, $j \neq f$.

The trip time is a good decision parameter because it indicates the appropriateness of the physical and logical

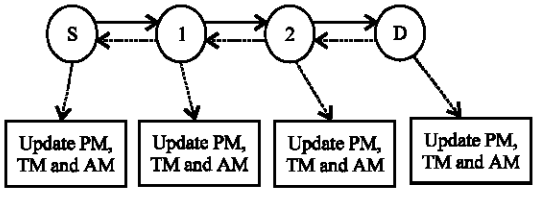

Fig. 1: Flow diagram of FA and BA

condition of the path which includes the number of hops, transmission capacity of the concerned link, processing time and queuing delay. A path with a high trip time also considered as a good path if its trip time is significantly lower than the other trip time.

In the data structures of the ACO, an additional secured model is added. The secured model will protect the entry of unauthorized mobile nodes. The security model is one byte information which copies the addrD information flooded in the route request and route reply which explained in the introduction. The addrD is the address of the destination which authorized. Based on the authorized entry of addrD, the initial secured model is defined. In addition to these routing information an additional flag is added for verifying the authentication and to avoid Denial of Service (DoS) attacks. The sequence number of each forward ant is added in the source node which again replicated when backward ant generated. The ants are piggybacked with every data packets. Hence, the duplicate communication injected by the attacker for DoS can be avoided.

The secured model is further updated with the values stored in the BA's memory. The time elapsed to arrive to the destination by the FA starting from the current node is used to update, according to the following equation:

$$\mu_i = \mu_i + \varsigma(RTT_{i\to d} - \mu_i) \quad (4)$$

$$\sigma_i^2 = \sigma_i^2 + \varsigma(RTT_{i\to d} - \mu_i)^2 - \sigma_i^2 \quad (5)$$

Where:

RTT_{i-d} = The new observed trip time from node i to the destination d

μ = The sample mean of the secured model

σ^2 = The variance of the secured model

ς = The representation of the weighs of the number of most recent samples that will really affect the average

The value of ς is calculated as $\varsigma = 0.1$ assuming that the latest fifty observations really influence the estimate (approximately), i.e., (5/50). Suppose 100 latest observations really influence the estimate then $\varsigma = 5/100 = 0.05$. The routing decision model computes and identifies the optimal path from the information stored in the data structures.

RESULTS AND DISCUSSION

The performance of proposed secured ACO routing are computed based on Good Forwarding Behaviou (GFB), Bad Forwarding Behaviour (BFB) and Security Trust (ST). The GFB and BFB are parameters which based on the throughput. The GFB represents packets transferred without loss due to attacks and BFB is vice-versa (Mohan and Baskaran, 2011b).

The BFB represents number of packet loss due to routing attacks. Hence, the throughput and packet loss due to routing attacks are compared in the Fig. 2-5.

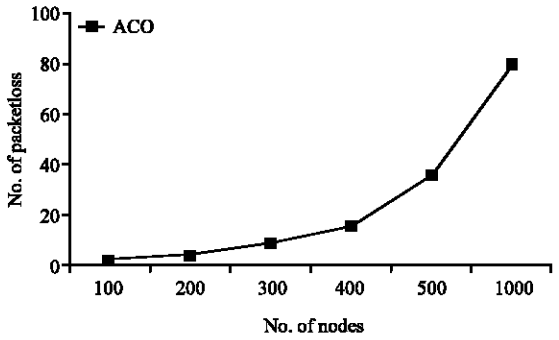

Fig. 2: Packetloss in ACO on no attack environment

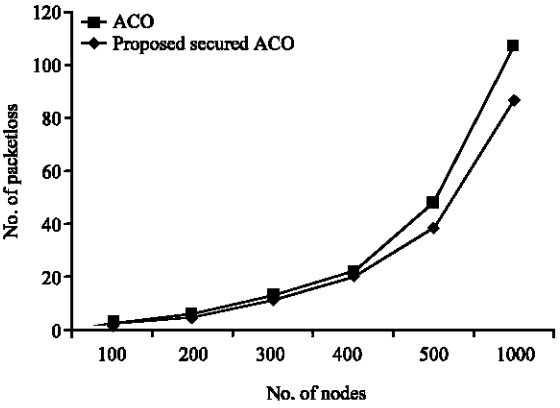

Fig. 3: Packetloss on ACO and secured ACO on simple injection attack

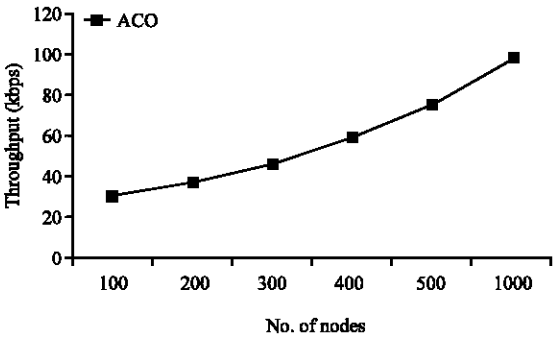

Fig. 4: Throughput in ACO on no attack environment

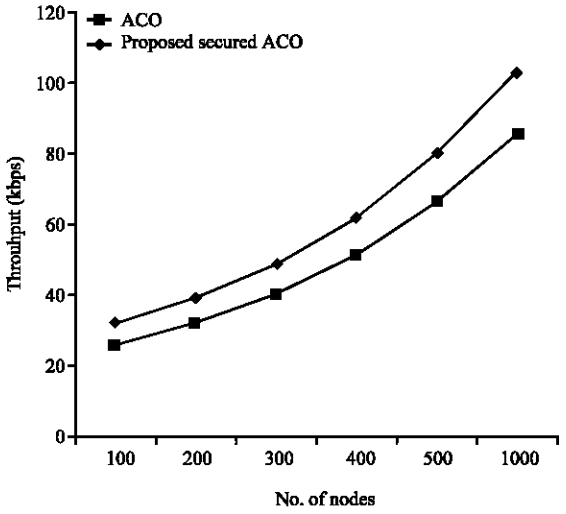

Fig. 5: Throughput on ACO and secured ACO on simple injection attack

In Fig. 2, the packet loss in ACO on no attack environment is shown. In Fig. 3, the packet loss on ACO and secured ACO on simple injection attack are shown. Similarly, the throughput in ACO on no attack environment is shown in Fig. 4 and the packet loss on ACO and secured ACO on simple injection attack are shown in Fig. 5.

CONCLUSION

The ACO proved as optimal routing in the wireless environment than traditional routing methods. Hence, securing ACO becomes important research issue for multi hop wireless network. The proposed secured ACO is compared with no attack and simple injection attack. The performance of secured ACO is computed on two metrics, packet loss and throughput. The packet loss shows the BFB behaviour and the throughput represents the GFB. From the result and performance analysis, it is concluded that the proposed secured ACO provides better result and improved the performance of ACO on both packet loss and consequent throughput.

REFERENCES

Arnold, M., M. Barron, M. Fritzsche and F. Nivelle, 1998. DREAM: data fusion and human factors applied to vehicle mounted mine detection. Proceedings of the 2nd International Conference on Detection of Abandoned Land Mines, October 12-14, 1998, Edinburgh, pp: 187-192.

Heinzelman, W.R., A. Chandrakasan and H. Balakrishnan, 2000. Energy-efficient communication protocol for wireless microsensor networks. Proceedings of the 33rd Hawaii International Conference on System Sciences, January 4-7, 2000, Washington, DC., USA. pp: 8020-8020.

Jacquet, P., P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, 2001. Optimized link state routing protocol for ad hoc networks. Proceedings of the 5th IEEE Multi Topic Conference, August 7, 2001, Springer, USA., pp: 62-68.

Joa-Ng, M. and I.T. Lu, 1999. A peer-to-peer zone-based two-level link state routing for mobile ad hoc networks. IEEE J. Sel. Areas Commun., 17: 1415-1425.

Johnson, D.B. and D.A. Maltz, 1996. Truly seamless wireless and mobile host networking. Protocols for adaptive wireless and mobile networking. IEEE Pers. Commun., 3: 34-42.

Manjeshwar, A. and D.P. Agrawal, 2001. TEEN: A routing protocol for enhanced efficiency in wireless sensor networks. Proceedings of the 15th International Parallel and Distributed Processing Symposium, April 23-27, San Francisco, California, USA., pp: 30189-30189.

Manjeshwar, A. and D.P. Agrawal, 2002. APTEEN: A hybrid protocol for efficient routing and comprehensive information retrieval in wireless sensor networks. Proceedings of the 16th International Parallel and Distributed Processing Symposium, April 15-19, 2002, Fort Lauderdale, FL., USA., pp: 195-202.

Mohan, B.C. and R. Baskaran, 2011a. Reliable transmission for network centric military networks. Eur. J. Sci. Res., 50: 564-574.

Mohan, B.C. and R. Baskaran, 2011b. Survey on recent research and implementation of ant colony optimization in various engineering applications. Int. J. Comput. Intell. Syst., 4: 566-582.

Mohan, B.C. and R. Baskaran, 2012. A survey: Ant colony optimization based recent research and implementation on several engineering domain. J. Exp. Syst. Appl., 39: 4618-4627.

Murthy S. and J.J., Garcia-Luna-Aceves, 1996. Congestion-oriented shortest multipath routing. Proceedings on IEEE Networking the Next Generation, March 24-28, 1996, San Francisco, CA., pp: 1028-1036.

Nikaein, N. H. Labiod and C. Bonnet, 2000. DDR-distributed dynamic routing algorithm for mobile ad hoc networks. Proceedings of the 1st Annual Workshop on Mobile and Ad Hoc Networking and Computing, August 11, 2000, Boston, MA., pp: 19-27.

Osipov, G.S., 2007. Workflows and their discovery from data. Proceedings of the International Conference on Integration of Knowledge Intensive Multi-Agent Systems, April 30-MAy 3, 2007, Waltham, MA., pp: 354-358.

Pearlman, H., 1998. The performance of a new routing protocol for the reconfigurable wireless networks. Proceedings of the IEEE International Conference on Communications, June 7-11, 1998, Atlanta, GA., pp: 156-160.

Perkins, C.E. and E.M. Royer, 1999. Ad-hoc on-demand distance vector routing. Proceedings of the 2nd Workshop on Mobile Computing Systems and Applications, February 25-26, 1999, New Orleans, LA., pp: 90-100.

Perkins, C.E. and P. Bhagwat, 1994. A mobile networking system based on Internet protocol. IEEE Personal Commun., 1: 32-41.