Macrothink Institute™

Network Protocols and Algorithms
ISSN 1943-3581
2011, Vol. 3, No. 4

MOBILE AGENT BASED ROUTING in MANETS – ATTACKS & DEFENCES

A. Radhika, Sr.Asst. Professor

Dept. of Computer Science

SRK Institute of Technology

Vijayawada, India

Email ID: radhisunil@yahoo.com

D. Kavitha, Sr.Asst Professor

Dept. of Information Technology

PVP Siddhartha Institute of Technology, Vijayawada, India

Email ID: kavitha_donepudi@yahoo.com

Dr. D. Haritha, Professor

Dept. of Computer Science

SRK Institute of Technology Vijayawada, India

Email ID: harithadasari@rediffmail.com

Received: December 11, 2011 Accepted: December 25, 2011 Published: December 31, 2011

DOI: 10.5296/npa.v3i4.1351 URL: http://dx.doi.org/10.5296/npa.v3i4.1351

Abstract

A Mobile Adhoc Network (Manet) is a highly challenging environment due to its dynamic topology, limited processing capability, limited storage, band width constraints, high bit error rate and lack of central control. In this dynamic network, each node is considered as a mobile router. A malicious node can easily disrupt the proper functioning of the routing by refusing to forward routing message (misbehavior node), inject the wrong routing packets, modifying routing information, etc. Hence the design of secured routing algorithm is a major issue in Manets. Mobile Agent based algorithms also called Ant Routing algorithms are a class of swarm intelligence and try to map the solution capability of ant colonies for routing in Manets. In this paper we discuss prominent attacks and propose counter-measures in three

Ant based routing protocols that are proactive, reactive and hybrid routing.

Keywords: Manets,Mobile Agents, Ant Routing, Security, AntNet , AntHocNet, ARA

1. Introduction

MANET is a communication network of a set of mobile nodes placed together in ad-hoc manner, in which nodes communicate via wireless link. All nodes have routing capabilities and forward data packets to other nodes in multi-hop transmission. Nodes can enter or leave the network at any time and may be mobile, so that the network topology continuously changes. Hence the primary challenge is to design effective routing algorithm that is adaptable to the changes in the behavior and topology of the MANETs.

Table-driven (proactive), on-demand (reactive) and hybrid routing protocols are three main categories of routing protocols for ad hoc wireless networks. Table driven routing algorithms include Destination Sequenced Distance Vector (DSDV), Clustered Gateway Switch Routing (CGSR) and Wireless Routing Protocol (WRP). On demand routing algorithms include Dynamic Source Routing (DSR), On-Demand Distance Vector Routing (AODV), Temporally Ordered Routing Algorithm (TORA) and Zone Routing Protocol (ZRP)[1]. Hybrid routing algorithms aim to use advantages of table driven and on demand algorithms and minimize their disadvantages. Ant colony Mobile agent based algorithms are a special category of algorithms (proactive, reactive and hybrid) that provide features such as adaptivity and robustness which essentially deal with the challenges of the MANETS.

Ant based algorithms [2][3] are the examples of swarm intelligence that can be applied to wide range of different optimization problems. They often give better results and turns out to be an appealing solution when routing becomes a crucial problem in a complex network scenario, where traditional routing techniques either fail completely or at least face intractable complexity. These algorithms are based on the study of ant colony behavior. In nature ants collectively solve the problems of cooperative efforts. Each individual ant performs a simple activity that has a random component. Collectively ants manage to perform several complicated tasks with high degree of consistency and adaptivity.

Ant based protocols for routing in Manets gather routing information through repetitive sampling of possible paths between source and destination nodes using artificial ant packets. Ants are biologically blind and thus communication between ants is indirect, in which they sense and follow a chemical substance called pheromone. Pheromone attracts the ants and therefore ants tend to follow trails that have higher pheromone concentration. As more ants use the route, they lay down more pheromone. As a result of this the shortest path emerges rapidly, because a shorter path has higher pheromone concentration, after which situation will converge where all other ants would follow only the trail which follows the strongest scent indicating the source out of possible routes from the colony nest to the food source (destination). This biological Ant-problem solving paradigm can be used to solve the routing problems in Manets by modeling an Ant colony as a society of mobile agents.

The Ant based algorithms are suitable for Manet routing because of the following properties:

A) Dynamic Topology

The Ant based algorithms are based on autonomous agent systems that allow the individual ants to develop a route. These algorithms are highly adaptable to change the topology of the network.

B) Local Work

In contrast to other routing approaches, the Ant algorithm is based on local information. No routing tables or other information blocks have to be transmitted to all other nodes of the network.

C) Link Paths and Support for multipath

It is possible to integrate the connector/link qualities in to the computation of the pheromone concentration, especially in the evaporate process. This will improve decision process with respect to link paths. Each node has routing table with entries for all its neighbors along with the destination and the corresponding pheromone concentration.

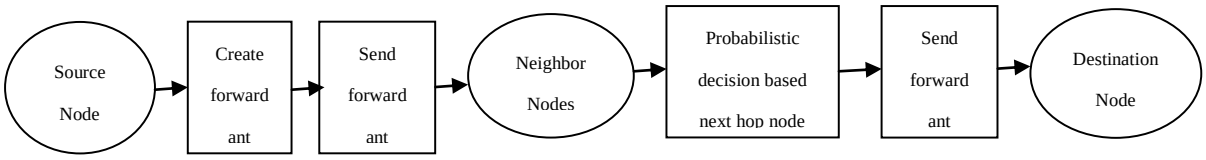

Figure 1 Transmission of forward ant

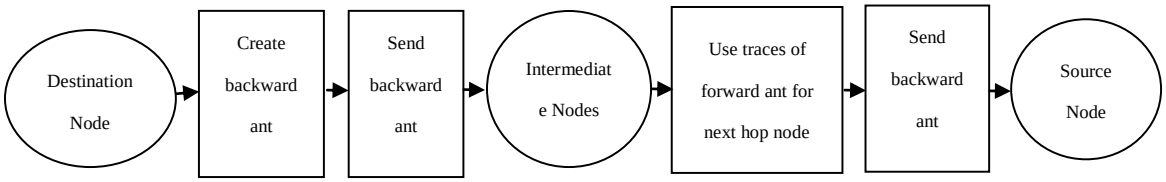

Figure 2 Transmission of backward ant

As shown in Fig 1. The source node creates a forward ant and sends the forward ant intended to route discovery to its neighbor nodes .Using Probabilistic decision it decides the next hop node and forward the forward ant through all the next hop nodes until it reaches the destination.

As in Fig 2 the destination node creates a backward ant and sends the backward ant in the same route traces made by the forward ant through the intermediate nodes until it reaches the source node.

Section 2 discusses the three Ant based Algorithms comprehensively. Various possible security attacks and their counter measures in the three algorithms are discussed in Section 3.

2. ANT COLONY OPTIMIZATION (ACO) BASED ROUTING ALGORITHMS

2.1. AntNet

It is a proactive routing algorithm proposed for wired datagram network based on the principle of ant colony optimization [4]. In Ant net each node maintains a routing table and has an additional task of maintaining the node movement statistics based on the traffic distribution over the network.

The routing table contains the destination node, next hop node and a measure of the goodness of using the next hop to forward data packet to the destination. The goodness measure is based on Pheromone values that are normalized to one. Ant net uses two sets of homogeneous mobile agents called forward ants and backward ants to update the routing tables. These mobile agents are small and light packets containing source IP address, destination IP address, packet ID and a dynamically growing stack consisting of Node ID and Node Traversal Time. A node which receives a forward ant for the first time creates a record in its routing table.

An entry in the routing table is having triple values. They are destination address, next hop and pheromone value. During the route finding process ants deposit pheromone on the edges.

In the simplest version of the algorithm, the ants deposit a constant amount $\Delta\psi$ of pheromone, i.e. the amount of pheromone of the edge ***e (i; j)*** when the ant is moving from node *i* to node *j* is changed as follows

$$\Psi i;j := \Psi i;j \quad +\Delta\psi \qquad (1)$$

The forward ant selects next node heuristically, based on pheromone value in the routing table. The forward ants are also used to collect information about traffic distribution over the network. When the forward ant reaches the destination, it generates the backward ant and then dies. The backward ant retraces the path of forward ant in the opposite direction. At each node backward ant updates the routing table and additional table containing statistics about traffic distribution over the network.

2.2 Ant Routing Algorithm (ARA)

It is a reactive protocol for mobile adhoc networks [5]. The routing table entries in ARA contain pheromone values for choosing a neighbor as the next hop for each destination, the pheromone values in the routing table decay with time and nodes enter a sleep mode if the

pheromone in the routing table has reached a lower threshold. Route discovery in ARA is performed by a set of two mobile agents forward ants and backward ants having unique sequential numbers, to prevent duplicate packet that are flooded through network by the source and destination nodes respectively .The forward ant and backward ant update the pheromone tables at the nodes along the path for source and destination respectively. Once the route discovery for a particular destination has been performed, the source node does not generate new mobile agents for the destination, instead the route maintenance is performed by the data packets.

In ARA ,the selection of next hop is decided by dynamic vs probabilistic routing .In Ant the selection of the next hop for a data packet is always decided by the amount of pheromone values, i.e. a node ***i*** selects a neighbor ***j*** with probability *P (i:j*) as follows

$$P_{i,j} = 1 \quad \text{if } \Psi_{i;j} \text{ is maximum}$$
$$0 \quad \text{otherwise} \qquad (2)$$

ARA is extended to use probabilistic routing, i.e. a node *i* selects a neighbor *j* with probability.

$$P_{ij} = \frac{\Psi_{i;j}}{\Sigma_{k \in Ni} \Psi_{i;j}} \qquad (3)$$

N_i is the set of one step neighbors of node *i*.

ARA with probabilistic routing is denoted by ARAstat. The main advantage of using probabilistic route selection is that the load is distributed over the existing paths to the destination.

*2.3. AntHocNet_*

AntHocNet is a hybrid algorithm [6]. It is reactive in the sense that a node only starts gathering routing information for a specific destination when a local traffic sensor needs to communicate with the destination and no routing information is available. In AntHocNet, nodes do not maintain routes to all possible destinations at all the times; rather the nodes generate mobile agents only at the beginning of a data session.

It is proactive because as soon as the communication starts and during the entire duration of the communication, the nodes proactively keep the routing information related to the ongoing flow up-to-date with network changes for both topology and traffic .The algorithm finds paths by minimal number of hops, low congestion and good signal quality between adjacent nodes.

Different Ant based Algorithms namely Ant Based Control Routing, Ant Colony based

Routing Algorithm Routing, Probabilistic Emergent Routing Algorithm, AntHocNet, AntNet were presented in [7]. Additional algorithms like Ant-AODV, Position based Ant Colony Routing Algorithm for MANETs (POSANT). Ant colony based Multi-path QoS-aware Routing (AMQR), Ant-based distributed route algorithm (ADRA). Ant routing algorithm for mobile ad hoc networks(ARAMA) were discussed in [8].However the algorithms working principles were presented but not in terms of their possible attacks and counter measures. Section 3 focusses on possible attacks and counter measures in AntNet,ARA and AntHocNet algorithms.

3. ATTACKS AND DEFENCES IN ANT ROUTING

Secured routing algorithms should be implemented in Mobile Adhoc networks due to the lack of pre deployed infrastructures, centralized policy and control. Malicious nodes can cause reduction of network traffic and DOS attacks by altering control message fields or by forwarding routing messages with falsified values.

The potential threats towards routing functions can be classified according to the attacker's goals:

a) Increase latency of particular packets,

b) Decrease overall network throughput,

c) Break down a particular node or link, or

d) Divert packets away from certain links to affect link bandwidth.

Security measures should be implemented in order to perform secure communications. The Ant routing algorithm does not incorporate any security mechanisms to protect and verify the information carried by ant agents. In a hostile environment, this makes it vulnerable to some attacks. The first study based on the study of the most basic attack possibilities available to an attacker who has compromised a node are to fabricate ant packets, to drop ant packets, or to tamper with information in ant packets.

3.1.Wormhole Attack

A wormhole [9] attack is one of the most sophisticated attacks in Manets mainly for reactive type of routing protocols such as AntHocNet and ARA routing algorithms. In this attack, a pair of attacker nodes creates tunnel between two groups of nodes. One attacker manages to receive the packet from one end of the tunnel and forwards them to another part of the network and relays them into the network from that point onwards. In reactive protocol this attack can be launched by tunneling every data packet transmitted towards the destination node. This is made possible by advertising high Pheromone values by the attacker nodes, while there is high data transmission link between them. So naturally the forward ant

will reach the destination first and hence the backward ant follows the same route i.e. through the attacker nodes. The attacker nodes may or may not modify the data packets.

For example in Fig. we assume that nodes M1 and M2 are two attackers. When a source node S sends a forward ant to its neighbor nodes B & E. Node M1 receive the forward ant forwarded by E tunnels the ant to another attacker node M2.Then the node M2 rebroadcast the ant to its neighbor H. Since this request is coming through high speed channel, this request will reach node D first. Therefore the node D chose the route as D-H-E-S and transmits the back ant to the source S and ignores the latter arrived forward ants initiated by S. As a result S will select the route as S-E-H-D.

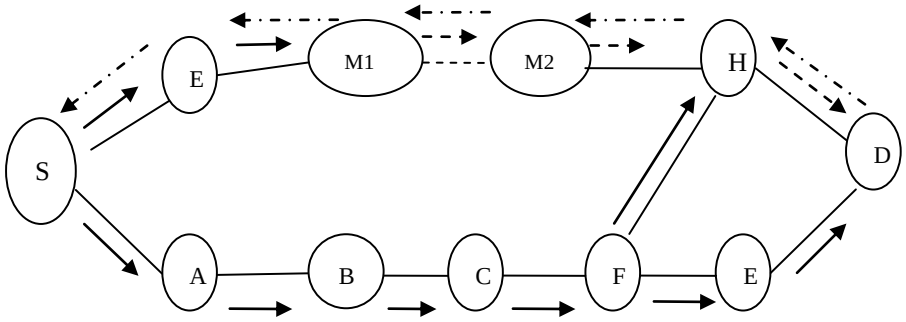

Figure 3 Wormhole Attack

These attacks can be detected by

- 1. Add two additional fields in the forward ant at every intermediate node, namely time of receipt of the forward ant t_{r1n} and time of release t_{r2n} of the forward ant to the next node in each hop.

  i.e. While the forward ant transmits through S->E->M1->M2->H->D at every intermediate nodes E,M1,M2,H the fields like $t_{r1E}\ t_{r2E}$, $t_{r1M1}\ t_{r2M1}$, $t_{r1M1}\ t_{r2M2}$, $t_{r1H}\ t_{r2H}$.

- The destination node has to verify the proportionality between the time taken in each hop i.e. difference between the time of receipt of the ant by the node and the time of release of the node by the previous node $(t_{r1M1-}\ t_{r2E})$ and the distance travelled at each hop to identify the attacker nodes.

- If there is abnormality, i.e if a pair of malicious nodes use high data transmission link, then the malicious nodes can be identified with the help of the dis- proportionality between the time taken in each hop and distance travelled at each hop. If there is no node to suspect, then the destination node can generate the backward ant to follow the same route.

3.2.Black hole Attack

Black hole attack [10] is one of the attacks in Manets mainly for proactive & reactive type of routing protocols such as AntNet, AntHocNet and ARA.

A malicious node sends fake routing information by giving high Pheromone value to reach the destination node and then claiming an optimum route and causes nodes to route packets through malicious node.

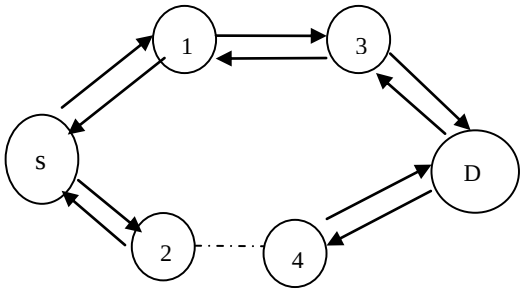

Figure 4 Blackhole Attack

For example, in Fig. 4, node S wants to send data packets to destination node D and initiates the route discovery process. We assume that node 2 is a malicious node and it claims that it has route to the destination whenever it receives route request packets, and immediately creates the back ant maliciously giving an assumption that it has all the way travelled from node D and sends that back ant to node S. If the response from the node 2 reaches first to node S then node S thinks that the route discovery is complete, ignores all other reply messages and begins to send data packets to node 2. As a result, all packets through the malicious node are consumed or lost.

The counter measure for the above attack is based on the trust and providing certification for all the genuine nodes in the network by the certification authority. If any malicious node enters into the network and advertizes high pheromone value, the forward ant selects that malicious node as its next hop node. It can be prevented by checking for certification of that node by the certification authority for its trust and then discards that node even though the node has highest pheromone value (as that node is not certified). The trust is computed as follows.

1. An additional data structure called Neighbors Trust *Table* is maintained by each network node.
2. Let $\{T_1, T_2, ...\}$ be the initial trust counters of the nodes $\{n1, n2, ...\}$ along the route R1 from a source S to the Destination D. Since the node does not have any information about the reliability of its neighbors in the beginning, next hop node can be selected based on only the pheromone value.
3. When a source S wants to establish a route to the destination D, it sends forward ant. When the destination D receives the forward ant, it sends backward ant to the source S.
4. The backward ant contains the list of intermediate nodes that come across the path from D to the node S. S first verifies that the first id of the route stored by the backward ant is its neighbor.

5. If it is true, then it verifies all the digital signatures of the intermediate nodes, in the backward ant. If all these verifications are successful, then the trust counter values of the nodes are incremented as

$$Ti = Ti + \Delta \tag{4}$$

If the verification is failed, then

$$Ti = Ti - \Delta \tag{5}$$

Where Δ is the step value, which can be assigned a small fractional value during the simulation.

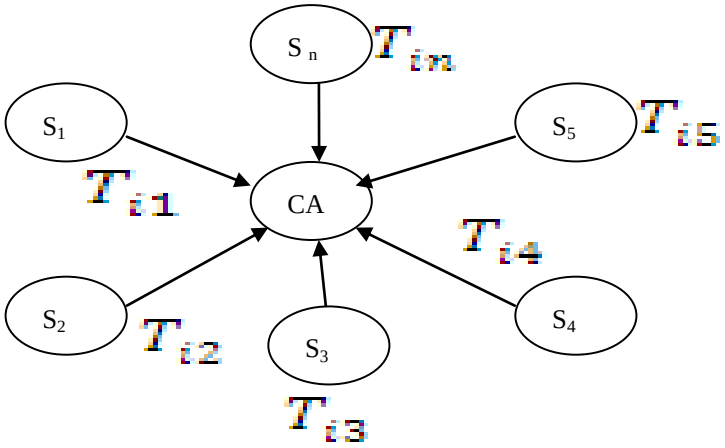

Figure 5 Trust calculation by CA

Source S_i transmits Trust table to the central certifying authority (CA). Likewise CA receives trust table from each source S_i and computes the trust factor for each node as the geometric mean of the trust factors of that node $\boldsymbol{n_i}$ by all the sources S_i.

$$T_i = \sqrt[n]{T_{i1}T_{i2}T_{i3}T_{i4}T_{in}} \tag{6}$$

If T_i is less than the minimum threshold value, then that node is considered and marked as malicious by the Certification Authority and that information is passed to all the nodes in that group.

3.3. Byzantine Attack

AntNet routing protocol is more vulnerable to Byzantine attack In this attack, a compromised intermediate node works alone or it works together with the other nodes and

carry out attacks such as creating routing loops, forwarding packets through non-optimal paths or selectively dropping packets which results in degradation of routing services[11].

In this method fault avoidance is carried out by a distributed process of learning free paths and the counter measure creates a routing process by adjusting the probability distribution at each node with neighboring nodes. The probability associated with forwarding and eventually neighbor reflects the relative likely hood of that neighbor delivering the packets to the destination.

3.4. Attacks using Fabrication

A Fabrication attack [12] is profoundly effects proactive & reactive type of routing protocols such as AntNet, AntHocNet and ARA.

Fabrication attack involves modification of the routing messages and transmitting the false routing messages. While selecting the next hop node the forward ant selects the node with high Pheromone value to the required destination and maintains the next hop node in the stack available with the forward ant. The malicious node purposefully falsifies the routing message by modifying the contents of the stack (which contains the information regarding the nodes through which the ant passed) available with the forward ant. Similarly the malicious node diverts the back ant by doing wrong manipulations on that stack. This attack can be avoided by ensuring that

1. Only one push operation can be done on the stack which is the identifier of that node in the forward path at each intermediate node.

2. Only one pop operation can be done on the stack which is the identifier of the next hop node at each intermediate node in the backward path.

3. In case of any link failure the node has to select the node having next higher Pheromone value as the next hop node .And the same must be notified to the certification authority.

4. Based on the confirmation from the certification authority about next node genuineness (trust) it continues with either the root discovery or the data transmission.

3.5. Denial-of-Service Attack

A Denial-of Service attack is one of the attacks in Manets that affects proactive type of routing protocols such as AntNet. It can be launched in AntNet by modifying the route of the forward ant i.e. altering the packet header thereby targeting to another destination. This leads to delivery of packets to the wrong destination. In the AntHocNet the attacker injects a large amount of junk packets into the network. These packets overspend a significant portion of network resources, and introduce wireless channel contention and network contention in the MANET. A routing table overflow attack and sleep deprivation attack are two other types of the DoS attacks. In the routing table overflow attack, an attacker attempts to create routes to nonexistent nodes.

Dos attack [13] can be handled by certifying the route signature for the created route containing source, destination and intermediate nodes by the certification authority. During the transmission of the data packets the nodes have to ensure the route signature. DOS attacks can be prevented from accessing the channel by outsider nodes. Routing table overflow attack can be avoided by restricting to only one push operation can be done in the forward path at each intermediate node and only one pop operation can be done at each intermediate node in the backward path.

3.6. Unauthorized Access by Impersonation Attack

Impersonation [14] is the ability to present credentials as if you are something or someone you are not. These attacks can take several forms: by capturing the data packets or recording an authorization sequence to replay at a later time. These attacks are commonly referred to as man-in-the-middle attacks, where an intruder is able to intercept traffic and can as a result hijack an existing session, alter the transmitted data, or inject bogus traffic into the network.

1. Source S creates Forward Ant and assume that the route taken by the Forward Ant to the destination D is S->A->B->C->D.
2. Destination D node creates Back Ant and adds its public key P_D in the Back Ant as an additional field.
3. Intermediate nodes C receives Back Ant and encrypts P_D with its public key P_C and forwards $P_C(P_D)$ along with the Back Ant to node B.Intermediate nodes B receives Back Ant and encrypts $P_C(P_D)$ with its public key P_B and forwards $P_B(P_C(P_D))$ along with the Back Ant to node A.
4. Intermediate nodes A receives Back Ant and encrypts $P_B(P_C(P_D))$ with its public key P_A and forwards $P_A(P_B(P_C(P_D)))$ along with the Back Ant to Source node S
5. Source node S receives Back Ant and $P_A(P_B(P_C(P_D)))$ and forwards data packets encrypted with the key $P_A(P_B(P_C(P_D)))$ in the traced route S->A->B->C->D.
6. All the intermediate node A receives the encrypted data packets and decrypts with its private key $P_A^{|}$ and forwards data packets encrypted with $P_B(P_C(P_D))$ to node B. In the similar manner all the intermediate decrypts with their private keys and forwards to next hop node.
7. Finally destination decrypts with its private key and accesses data packets. Thus the attacker or intruder cannot enter into the network if that node is not participated in the route discovery phase. However the malicious nodes must be taken care by the certification authority.

All the above mentioned attacks and defences are summarized in the Table1 given below.

Table1 Comparison of Attacks & Defenses in three Ant Routing Algorithms

Types of Attack	Attack	Defences	Routing Algorithm effected
Worm Hole	A pair of attacker nodes creates tunnel between two groups of nodes	Add two additional fields, time of receipt of the forward ant t_{r1n} and time of release t_{r2n} of the forward ant to the next node in each hop.	AntHocNet ARA
Black Hole	Fake routing information by advertising high Pheromone	1)Certifying all the genuine nodes 2) An additional Neighbors Trust *Table* is maintained by each node.	AntNet, AntHocNet and ARA
Byzantine	Creating routing loops, forwarding packets through non-optimal paths or selectively dropping packets	A distributed process of learning free paths and by adjusting the probability distribution of delivering the packets to the destination by each neighboring node .	AntNet
Fabrication	1)Modification/False transmission of the routing messages by modifying the contents of the stack. available with forward Ant 2) Diverting the back ant by doing wrong manipulations on that stack.	Allowing only one push operation on stack in the forward path and one pop operation in the backward path.	AntNet, AntHocNet and ARA.
Denial-of Service Attack	1)Modifying the packet header 2) Inducing Junk packets into the network. 3)Routing table overflow	1)Certifying the route signature 2)Monitoring no of packets released by each node 3)Allowing only one push operation on stack in the forward path and one pop operation in the backward path.	AntNet, AntHocNet and ARA.
Impersonation	1)Capture the data packets 2) intercept traffic and can hijack an existing session, alter the transmitted data, or inject bogus traffic into the network.	Public key of destination in the Back Ant is encrypted by public keys of each node during its path to source and is used to encrypt the data packets by the source.	AntNet, AntHocNet and ARA

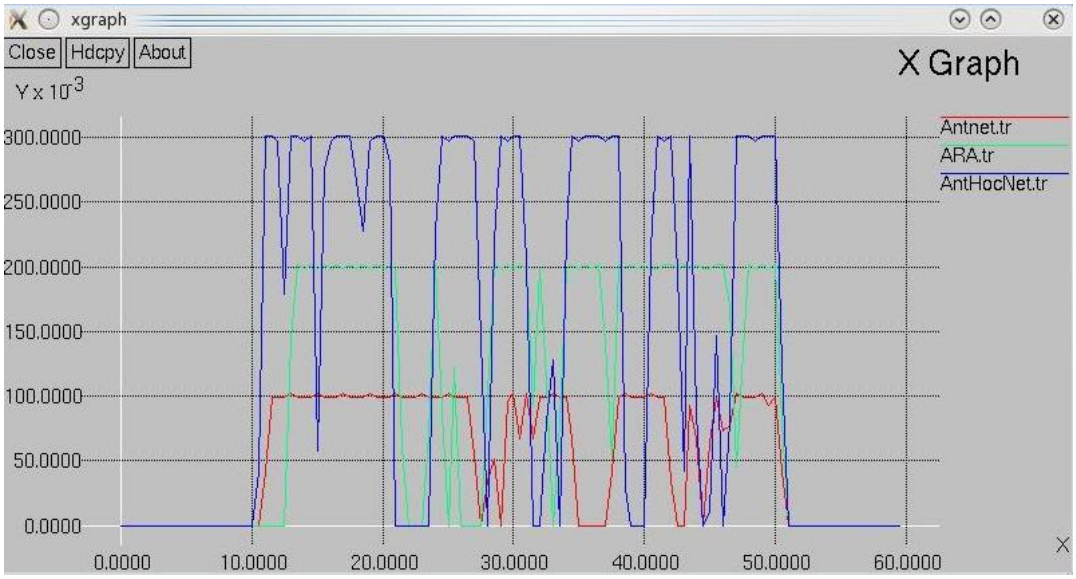

Figure 6 Throughput of Ant Routing Algorithms

The performance of these routing algorithms and counter measures given in this paper is analyzed on NS-2 simulator and observed to offer better preliminary results. The results are analyzed in terms of Throughput, Packet Delivery Ratio, End to End Delay, Packet Latency, Route Link Failure and Recovery Speed. Figure 6 shows the throughput analysis of three ant routing algorithms. However a detailed analysis is to be done to compare the performance of these algorithms and counter measures.

4. CONCLUSION

Ant colony algorithms tend to provide features such as adaptivity and robustness which essentially deal with the challenges of the MANETS. Ant routing algorithms for Manets considered in this paper are prone to different attacks. We suggested the counter measures for more prominent attacks in Ant Routing algorithms. Authentication mechanisms and certification provided by trusted authority will defend against these attacks to a certain extent, but careful design against these attacks is to be still developed. The analysis given in this paper can be extended to design more robust and secured Ant routing protocol.

5. REFERENCES

[1] Radwan, A.A.A.; Mahmoud, T.M.; Hussein, E.H, " AntNet-RSLR: A Proposed Ant Routing Protocol for MANETs", Electronics, Communications and Photonics Conference (SIECPC), 24-26 April 2011, pp 1–6, 2011, http://dx.doi.org/10.1109/SIECPC.2011.5876984

[2] Colorni, A., Dorigo M. & Maniezzo V.,"The Ant System: Optimization by a colony of co- operating agents", IEEE Transactions on Systems, Man, and Cybernetics-part B, Vol. 26, No.1, pp.1-13, 1996. http://dx.doi.org/10.1109/3477.484436.

[3] Mikkel Bundgaard, Troels C. Damgaard, Federico Decara og Jacob W. Winther, "Ant Routing System". Springer 2002 IT University of Copenhagen-Internet Technology.

[4] Gianni Di Caro and Marco Dorigo, "AntNet: distributed stigmergetic control for communication networks", Journal of Artificial Intelligence Research, vol. 9, pp. 317-365, 1998.

[5] Mesut Gunes and Otto Spaniel, "Routing algorithms for mobile multihop ad-hoc networks", Conference on Network Control and Engineering for QoS (Net-Con 2003), pp. 120-138, 2003.

[6] Gianni Di Caro, Frederick Ducatelle and Luca Maria Gambardella, "AntHocNet: an adaptive nature-inspired algorithm for routing in mobile ad hoc networks", European Transactions on Telecommunication, Volume 16, pp: 443-455, 2005. http://dx.doi.org/10.1002/ett.1062

[7] Brijesh Bhatt Vasundhara Uchhula. "Comparison of different Ant Colony Based Routing Algorithms". *International Journal of Computer Applications (IJCA).* Vol. 2. Pp. 97–101, 2010. http://dx.doi.org/10.5120/1040-65.

[8] Kalaavathi, B.; Madhavi, S.; VijayaRagavan, S.; Duraiswamy, K.;" Review of ant based routing protocols for MANET" Proceedings of the 2008 International Conference on Computing, Communication and Networking (ICCCN 2008). http://dx.doi.org/10.1109/ICCCNET.2008.4787667

[9] Y-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks", IEEE JSAC, vol. 24, no. 2, Feb. 2006, http://dx.doi.org/10.1109/JSAC.2005.861394.

[10] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kato, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, Vol. 5, No. 3, Pp. 338–346, Nov. 2007.

[11] B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-demand Secure Routing Protocol Resilient to Byzantine Failures". Proceedings of the ACM Workshop on Wireless Security, pp. 21-30, 2002.

[12] S. Desilva, and R. V. Boppana, "Mitigating Malicious Control Packet Floods in Ad Hoc Networks," Proc. IEEE Wireless Commun. and Networking Conf., New Orleans, LA, pages 2112 - 2117 ,Vol. 4, 2005, http://dx.doi.org/10.1109/WCNC.2005.1424844.

[13] L. Zhou and Z. J. Haas. "Securing Ad Hoc Networks". IEEE Network Magazine, Volume. 13, no. 6, Pages 24-30, December 1999. http://dx.doi.org/10.1109/65.806983

[14] Dimitris Glynos, "Preventing Impersonation Attacks in Manet with Multi- factor Authentication", Proceeding of the Third International Symposium on Modeling and Optimization in Mobile Adhoc and Wireless Networks, no 6, pages 59-64, IEEE 2005. http://dx.doi.org/10.1109/WIOPT.2005.42

Copyright Disclaimer