Detection and Prevention of Blackhole Attack in MANET Using ACO

Sowmya K.S, Rakesh T. and Deepthi P Hudedagaddi

Dept. Of Computer Science and Engineering,Visvesvaraya Technological University,Belgaum,Karnataka,India

Summary

With the increase in use of MANETS, security has become an essential requirement to provide protected communication between mobile nodes. To overcome the challenges, there is a need to build a multifence security solution that achieves both broad protection and desirable network performance. MANETs are vulnerable to various attacks. Blackhole is one of the possible attacks. Black hole is a type of routing attack where a malicious node advertises itself as having the shortest path to all nodes in the environment by sending fake route reply. By doing this, the malicious node can deprive the traffic from the source node. It can be used as a denial-of-service attack where it can drop the packets later. In section 1, we have given introduction about MANET and brief description of attacks in MANET. Section 2 deals with background of Ant Colony Optimization(ACO). Section 3 tells about ANT NET, where ACO system and pseudocode of it has been proposed. The most important part of our paper is section 4 where we proposed a method to detect and prevent blackhole attacks by notifying other nodes in the network of the incident. Section 5 and 6 tells about applications and conclusion respectively. Our protocol not only prevents blackhole attack but consequently improves the overall performance of (normal) ACO in presence of black hole attack.

Key words:

MANETs, ACO, Routing protocol, blackhole attack.

1. Introduction

A mobile ad hoc network (MANET) is relatively new communication paradigm. MANET has received spectacular consideration because of their self-configuration and self-maintenance. Early research assumed a friendly and cooperative environment of wireless network. As a result they focused on problems such as wireless channel access and multihop routing.

But security has become a primary concern to provide protected communication between mobile nodes in a hostile environment. Although mobile ad hoc networks have several advantages over wired networks, on the other side they pose a number of non-trivial challenges to the security design as they are more vulnerable than wired networks [1]. These challenges include open network architecture, shared wireless medium, demanding resource constraints, and, highly dynamic network topology.

In this paper, we have considered a fundamental security problem in MANET to protect its basic functionality to deliver data bits from one node to another. Nodes help each other in conveying information to and fro and thereby creating a virtual set of connections between each other. Routing protocols play an very imperative role in the creation and maintenance of these connections.

In contrast to wired networks, each node in an ad-hoc networks acts like a router and forwards packets to other peer nodes. The wireless channel is accessible to both legitimate network users and malicious attackers. As a result, there is a blurry boundary separating the inside network from the outside world.

Many different types of routing protocols have been developed for ad hoc networks and have been classified into two main categories by Royer and Toh (1999) as Proactive (periodic) protocols and Reactive (on-demand) protocols which has been clearly explained in [2] and [3]. Wireless ad hoc networks are vulnerable to various attacks. These include passive eavesdropping, active interfering, impersonation, and denial-of-service. A single solution cannot resolve all the different types of attacks in ad hoc networks. In this paper, we have designed a novel method to detect blackhole attack: ACO, which isolates that malicious node from the network. We have complemented the reactive system on every node on the network. This agent stores the Destination sequence number of incoming route reply packets in the routing table and calculates the threshold value to evaluate the dynamic training data in every time interval as in [4]. Our solution makes the participating nodes realize that, one of their neighbors is malicious; the node thereafter is not allowed to participate in packet forwarding operation[5].

2. Theoretical Background of ACO

The basic principle of an ant routing algorithm is that ants deposit on the ground a hormone, the pheromone, while they roam looking for food. Ants can also smell pheromone and tend to follow with higher probability those paths characterized by strong pheromone concentrations. The pheromone trails allow the ants to

Manuscript received May 5, 2012
Manuscript revised May 20, 2012

find their way to the food source (or back to the nest). The same pheromone trails can be used by other ants to find the location of the food sources discovered by their nest mates. It was demonstrated experimentally that this pheromone-trail-following behaviour gives raise to the emergence of the shortest path.
An ant routing algorithm can be briefly described in the following way in Fig. 1

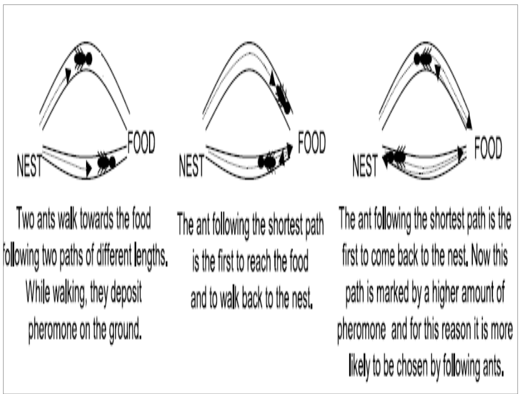

Fig 1 : Basic principle of ant routing paradigm.

From each network node, a number of discovery packets (forward ants) are sent towards the selected destination nodes. They propagate concurrently and independently. In each node routing tables consists of stochastic tables, used to select next hops according to weighted probabilities. These probabilities are calculated on the basis of the pheromone trails left by previous ants which is as shown below:

Destination node	1	...	j	...	k-1	k+1	...	N
Next node	l_1	...	l_j	...	l_{k-1}	l_{k+1}	...	l_N

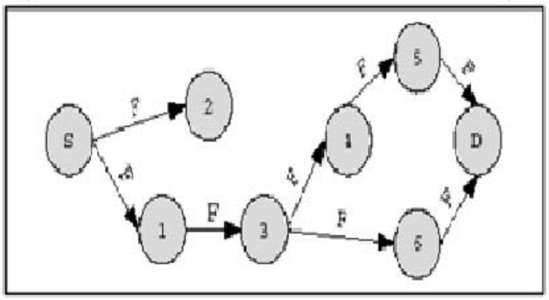

Fig 2 : Routing Tables

Ant's Pheromone trail depositing

$$\tau_{ijd}^{k}(t+1) \leftarrow (1-\rho)\cdot \tau_{ijd}^{k}(t) + \Delta\tau_{ijd}^{k}(t)$$

where the (i,j)'s are the links visited by ant k, and

$$\Delta\tau_{ijd}^{k}(t) = quality^{k}$$

where quality k is set proportional to the inverse of the time taken by ant k to build the path from i to d via j which is shown in Fig 3[7].

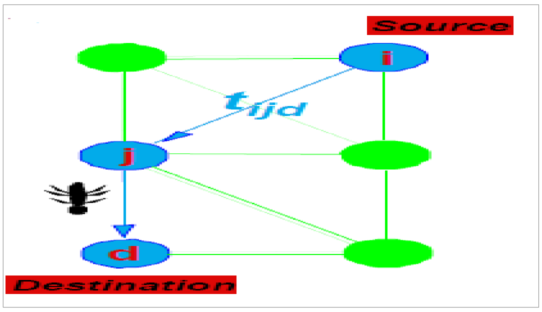

Fig 3 : Trail depositing

While moving, the ants deposit pheromone on the path links, i.e., in the node routing tables they change the probability to select a particular next hop.
Once a forward ant gets to the destination node, it first generates a backward ant and then dies. This way, the new packet created and sent back to the source will propagate through the same path selected by the forward ant.
On its way back, the backward ant deposits pheromone on the reverse path links. Thus it updates the routing table of the nodes along the path. Once it has returned to the source node, the backward ant dies. A distributed heuristic solution like the ant routing displays several features making it particularly suitable in ad hoc networks[6].
However research has shown that in MANETs , the best path for routing (considering the overall network benefit as well as node benefit) is not necessarily the shortest path but instead the path which optimizes number of hops (length of path), congestion along path and load balancing[8].

3. ANT NET

AntNet is an instance of an ACO algorithm for distributed and adaptive routing in communications networks. In distributed adaptive routing at each network node the routing policy is continually adapted to the variations in the input traffic patterns. A routing policy is a local mapping parameterized by a data structure called routing table. It is assumed that a robust model of the input traffic is not available: the policy should be learned[7].

3.1 Ant Colony Optimization(ACO) System

- Starting node is selected at random.
- Path is selected randomly based upon:
  - amount of “trail” present on possible paths from starting node.
  - higher probability for paths with more “trail”.
- Ant reaches next node, selects next path.
- Continues until reaches starting node.
- Finished “tour” is a solution.
- A completed tour is analyzed for optimality.
- Higher probability of ant selecting path that is part of a better-performing tour.
  - New cycle is performed.
- Repeated until most ants select the same tour on every cycle (convergence to solution).

4. ATTACKS IN MANETS

MANETs are vulnerable to various attacks. General attack types are the threats against Physical, MAC, and network layer which are the most important layers that function for the routing mechanism of the ad hoc network. Attacks in the network layer have generally two purposes: not forwarding the packets or adding and changing some parameters of routing messages. Black hole is one of the major threat.

4.1 Blackhole Attack

In blackhole attack, the malicious node waits for the neighbors to initiate a FORWARD ANT packet. As the node receives the FORWARD ANT packet, it will immediately send a false BACKWARD ANT packet with a modified higher sequence number. So, that the source node assumes that node is having the fresh route towards the destination. The source node ignores the BACKWARD ANT packet received from other nodes and begins to send the data packets over malicious node. A malicious node takes all the routes towards itself. It does not allow forwarding any packet anywhere. This attack is called a blackhole as it swallows all objects[9].

In figure 4 source node S wants to send data packets to a destination node D in the network.

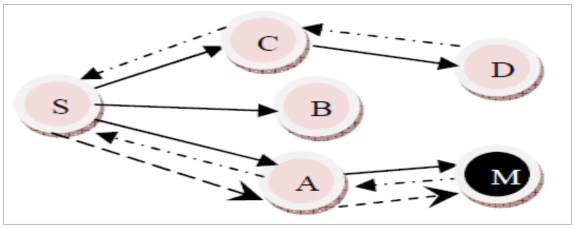

Fig 4 Blackhole attacks in MANETs

Node M is a malicious node which acts as a blackhole. The attacker replies with false reply BACKWARD ANT having higher modified sequence number. So, data communication initiates from S towards M instead of D.

4.2 Solution Against Blackhole Attack

In normal ACO, the node that receives the BACKWARD ANT packet first checks the value of sequence number in its routing table. The BACKWARD ANT packet is accepted if it has BACKWARD_ANT_sequence number higher than the one in routing table. Our solution does an addition check to find whether the BACKWARD_ANT_sequence_number is higher than the threshold value. The threshold value is dynamically updated as in [4] in every time interval. As the value of BACKWARD ANT_sequence_number is found to be higher than the threshold value, the node is suspected to be malicious and it adds the node to the black list. As the node detected an anomaly, it sends a new control packet, ALARM to its neighbours. The ALARM packet has the black list node as a parameter so that, the neighbouring nodes know that BACKWARD ANT packet from the node is to be discarded. Further, if any node receives the BACKWARD ANT packet, it looks over the list, if the reply is from the blacklisted node; no processing is done for the same. It simply ignores the node and does not receive reply from that node again. So, in this way, the malicious node is isolated from the network by the ALARM packet. The continuous replies from the malicious node are blocked, which results in less routing overhead. Moreover, unlike ACO, if the node is found to be malicious, the routing table for that node is not updated, nor the packet is forwarded to another node.

The threshold value is dynamically updated using the data collected in the time interval. If the initial training data were used, then the system could not adapt the changing environment. The threshold value is the average of the difference of destination _sequence_number in each time slot between the sequence number in the routing table and the BACKWARD ANT packet. The time interval to update the threshold value is as soon as a newer node receives a BACKWARD ANT packet. As a new node receives a BACKWARD ANT for the first time, it gets the updated value of the threshold. So our design not only detects the blackhole attack, but tries to prevent it further, by updating threshold which reflects the real changing environment. Other nodes are also updated about the malicious act by an ALARM packet, and they react to it by isolating the malicious node from network.

5. APPLICATIONS

Ad-hoc networks are suited for use in situations where an infrastructure is unavailable or to deploy one is not cost effective. One of many possible uses of mobile ad-hoc networks is in some business environments, where the need for collaborative computing might be more important outside the office environment than inside, such as in a business meeting outside the office to brief clients on a given assignment. Work has been going on to introduce the fundamental concepts of game theory and its applications in telecommunications. A mobile ad-hoc network can also be used to provide crisis management services applications, such as in disaster recovery, where the entire communication infrastructure is destroyed and resorting communication quickly is crucial. By using a mobile ad-hoc network, an infrastructure could be set up in hours instead of weeks, as is required in the case of wired line communication. Another application example of a mobile ad-hoc network is Bluetooth, which is designed to support a personal area network by eliminating the need of wires between various devices, such as printers and personal digital assistants.

6. CONCLUSION

In this paper, we have used a very simple and effective way of providing security against blackhole attack by introducing some modifications
to ACO. The ACO algorithm is efficient in providing an optimal path for the reasons like, it is fully distributed implies there is no single point of failure; the operations to be performed in each node are very simple; the algorithm is based on an asynchronous and autonomous interaction of agents; it is self-organizing, thus robust and fault tolerant implies there is no need of defining path recovery algorithms; it is intrinsically traffic adaptive without any need for complex and yet inflexible metrics; it is inherently adaptive to all kinds of long-term variations in topology and traffic demand, which are difficult to be taken into account by deterministic approaches. By adding a threshold value factor to ACO, the black hole attack is not only detected, but also prevented. Hence, by using ACO(with threshold value factor) as a routing algorithm in MANETS, one can also be sure of not being susceptible to black hole attacks. Our prevention scheme detects the malicious nodes and isolates it from the active data forwarding and routing and reacts by sending ALARM packet to its neighbors.We also infer that a more detailed research and with some add-on features to ACO, the other security threats can also be detected and to a certain extent prevented like the way we have proposed for the black hole attack.

REFERENCES

[1] Hao Yang, Haiyun Luo. Fan Ye, Songwu Lu, and Lixia Zhang. "Security in mobile ad hoc networks: Challenges and solutions". IEEE Wireless Communications , February 2004

[2] Shree Murthy and J. J. Garcia-Luna-Aceves. "An Efficient Routing Protocol for Wireless Networks". Mobile Networks and Applications, 1(2):183–197, 1996.

[3] Charles E. Perkins and Elizabeth M. Royer. "Ad-Hoc On- Demand Distance Vector Routing". In Proceedings of the Second IEEE Workshop on Mobile Computing Systems and Applications (WMCSA'99), pages 90–100, February 1999.

[4] Satoshi Kurosawa, Hidehisa Nakayama, Nei Kat, Abbas Jamalipour, and Yoshiaki Nemoto, "Detecting Blackhole Attack on ACO-based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security, Vol.5, No.3, P.P 338-346, Nov. 2007

[5] Laura Rosati Matteo Berioli, Gianluca Reali,´" On ant routing algorithms in ad hoc networks with critical connectivity", _ 2007 Elsevier B.V Journal - 2007

[6] Luca Maria Gambardella IDSIA, Lugano, "Ant Colony Optimization for ad-hoc networks", The First MICS Workshop on Routing for Mobile Ad-Hoc Networks Zurich, February 13, 2003, 14:00-17:00, ETH-Room ETZ E8

[7] Ajay C Solai Jawahar Department of Electrical Engineering,Rutgersajaychak@eden.rutgers.edu,"Ant Colony Optimization for Mobile Ad-hoc Networks"

[8] Dokurer, Semih."Simulation of Black hole attack in wireless Ad-hoc networks". Master's thesis, AtılımUniversity, September 2006

Sowmya K S received B.E. degree in Computer Science and Engineering from SJMIT, Kuvempu University in 2001 and M.Tech from DSCE, VTU in 2008. Her research interest includes routing and security in WSN and MANETS. She is currently working as a Lecturer at Dayananda sagar college of engineering.

He is pursuing his B.E at Visveswaraya Technological University, Belgaum, India. He is currently in third year of Dept. of Computer Science and Engineering, DSCE. He is a member of Computer Society of India. His research interests include routing in Manets and preventing the possible attacks in Manets.

She is pursuing her B.E at Visveswaraya Technological University, Belgaum, India. She is currently in third year of Dept. of Computer Science and Engineering, DSCE. She is a member of Computer Society of India. Her research interests include routing in Manets and preventing the possible attacks in Manets.