Volume 4, Issue 8, August 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Improving AODV Protocol by Nature Inspired Technique Against Blackhole and Greyhole Attacks in MANETs

Manita*	Prof(DR.) Vinay Kumar Nassa	Mr. Kapil Chawla
M.Tech (CSE)	Director-Principal	Assistant Professor
SITM, Sonepat, India	SITM, Sonepat, India	SITM, Sonepat, India

Abstract- An Ad hoc network is the network with no fixed infrastructure. There is no central administrator so any node can comeand move in and outside of the network in a dynamic manner. This makes it more dynamic and complex which makes it moreprone to attacks. In this paper the AODV protocol is modified to handle the blackhole attack and greyhole attack. The ACO is used to modify the AODV routing protocol. The ant place of at each node calculates its pheromone value by using the forwarding ratio at node. This modified protocol is compared with existing protocol by using various parameters i.e. pdr, e2edelay and throughput. The increase in pdr, throughput and decrease in e2edelay show better performance of proposed work as compared existing.

Keywords— MANET, Grey hole attack, Black hole attack, Routing Protocols, security, Ant colony technique, AODV

I. INTRODUCTION

Mobile Ad-hoc Network is a group of mobile nodes without any fixed infrastructure therefore the nodes communicate with each other based on the unconditional trust. The security is more complicated in MANET when compared with ordinary network which the intruder may get physical access to the wired link or pass over security holes at firewalls and routers [1]. Mobile ad hoc network does not have a well-defined line of protection due to its infrastructure-free and each node shall be prepared for any threat. In wireless ad-hoc networks, the most important concern is routing issues. These protocols suffer various attacks that advertise themselves in the entire network. (i.e. black hole attack, worm hole attack, gray hole attack, etc). In this paper, we analyse and detect the black hole attack as well as grey hole attack. To detect the black hole attack and grey hole we proposed an algorithm using ant colony technique.

A. Routing Protocols

There are various routing protocols in MANET which are categorized in term of functionality as following: reactive protocols, proactive protocols and hybrid protocol. Reactive protocols are known as On Demand Reactive protocols which never initiate route discovery, unless they are requested by a source node. Proactive routing protocols maintain the updated topology of the network and each node knows the other nodes in the network in advance. Hybrid protocol is created by exploiting the benefits of both reactive and proactive protocols which could be used to achieve better results. We use AODV protocol. AODV is reactive protocol Routing information is collected only when it is needed, and route determination depends on sending route queries throughout the network. When a route to a new destination is needed, the node broadcasts a RREQto find a route to the destination. Each node receiving the request caches a route back to the originator of the request, so that the RREP can be unicast from the destination along a path to that originator[2].

B. Black hole attack

A black hole node that attracts all the packets by falsely claiming that it has valid route to destination node. It disturbs the routing protocol by deceiving other nodes about the routing information. A black hole node works in the following scheme: once receiving RREQ messages, the attacker replies RREP messages directly and claims that it is the destination node or had valid route to destination node. Under these circumstances, the source node sends data packets to the black hole instead of the destination node. When the source node transmits data packets through the black hole, the attacker discards them without sending back a RERR message [2].

C. Gray hole attack

Gray hole attack is an attack in which some selective data packets are dropped by the malicious node. Gray hole attack is harder to find because of some data packets reached the destination and destination thinks that it is getting the full data. Example, Dropping all UDP packets while forwarding TCP packets, Dropping 50% of the packets or dropping them with a probabilistic distribution. These are the attacks that seek to disrupt the network without being detected by the security measures.

D. Nature Inspired Techniques

Nature-inspired meta heuristic algorithms are becoming popular and powerful in solving optimization problems [3]. A wide range of nature-inspired algorithms have emerged over the last few decades. The simulated annealing (SA) algorithm was developed by modelling the steel annealing process. The ant colony optimization (ACO) was inspired from the behavior of a real ant colony, which is able to find the shortest path between its nest and a food source. The particle swarm optimization (PSO) algorithm was developed based on the swarm behavior, such as fish and bird schooling in nature.

E. Ant Colony Technique

Ants are social insects that live in colonies and, because of their collaborative interaction; they are capable of showing complex behaviors and to perform difficult tasks from an ant's local perspective. A very interesting aspect of the behaviour of several ant species is their ability to find shortest paths between the ants' nest and the food sources. This fact is specially noticeable having in mind that in many ant species ants are almost blind, which avoids the exploitation of visual clues. This behaviour also allows ants to identify shortest paths between their nest and a food source [4]. We use this ant colony technique to modify the AODV protocol to in the performance of network.

II. LITERATURE REVIEW

Seungjoon Lee et al. [5] (2002) proposed a scheme that strengthens robustness of routing information in ad hoc networks. It introduces additional route confirmation request and response messages, and is interoperable with most existing on demand routing protocols. Simulation results validate the effectiveness of our protocol against blackhole attack. With malicious nodes, delivery ratio of their protocol stays as high as 80% while DSR delivers less than 50% of data packets sent. Data transmission overhead is also reduced by 10% compared to DSR, and in case of no malicious attempt, our protocol incurs only 5% additional control overhead.

SemihDokurer et al. [6] (2007) analyzed the effects of black holes in ad-hoc networks.They implemented an AODV protocol that simulates the behavior of a black hole in ns-2 and they simulated 100 scenarios each involving different ad-hoc networks with 20 nodes each moving randomly. They introduced a black hole in each scenario and compared the performance of the networks with and without a black hole. They also tested a network with two black holes for only five scenarios. They then implemented a modified AODV protocol which responded to the second RREP message if it arrived assuming that it is more likely to have the first RREP arriving from the black hole if one exists in the network.

Rutvij H. Jhaveri et al. [7] (2012) proposed a scheme for Ad-hoc On-demand Distance Vector (AODV) protocol, in which an intermediate node detects the malicious node sending false routing information; routing packets were used not only to pass routing information, but also to pass information about malicious nodes. The proposed scheme not only detects but also removes malicious node by isolating it, to make safe and secure communication.

WatcharaSaetang et al. [8] (2012) proposed CAODV, according to the nature of AODV routing protocol in ad hoc networks, the black hole attack is able to harm and decrease a throughput of network, especially in the route discovery phase. By using a credit mechanism, we can detect and protect a malicious node before the black hole attack is occurred. We have successful demonstrated that the black hole cannot attack the networks when our CAODV is employed. In contrast with CAODV, we found the average throughput of the original AODV is decreased at about 40 percentages when the network is attacked by the black hole.

ChuanhaoQu, Lei Ju et al. [9] (2013) proposed a novel trust model with an intrusion detection system by detecting malicious dropping packet behavior. As an application of the model, we extended the AOMDV to a light-weight trust-based multipath routing protocol called LWT-AOMDV. This new protocol could establish multiple trustworthy paths and launch a route handoff when detecting paths with malicious nodes. This approach could reduce the buffer size and alleviate the computation overhead by using two timmers. Three metrics to evaluate the performance of these routing protocols in which the first two metrics especially the delivery ratio are important for the service quality and the third could reflect the scalability of the approach.

III. PROPOSED WORK

The existing algorithm detect the black hole attack. In this work the AODV protocol is modified to detect and recover the grey hole as well as the black hole attack. The AODV is modified by using the ant colony optimization. The working steps of the algorithm are given below:

```
1. Select  source node and destination node
2. Place Ant at each node in the network
3. Pheromone value at node = forwarding ratio at node = transfer of data packets at receiver/ transfer of data packets at
   sender
4. Current_node = S
5. While current_node ! = Destination
6. Broadcast current_node
7. node with highest Pheromone value
8. Forward the packets
9. Update current_node
10. End while
```

IV. PARAMETER ANALYZED

The algorithm specified in the section 3 is analyzed by using the following parameters.

A. Packet Delivery Ratio

The ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination .

∑ Number of packet receive / ∑ Number of packet send

The greater value of packet delivery ratio means the better performance of the protocol.

B. End-to-end Delay

The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

∑ (arrive time – send time) / ∑ Number of connections

C. Throughput

Throughput refers to how much data can be transferred from one location to another in a given amount of time. It is used to measure the performance of hard drives and RAM, as well as Internet and network connections. For example, a hard drive that has a maximum transfer rate of 100 Mbps has twice the throughput of a drive that can only transfer data at 50 Mbps. Similarly, a 54 Mbps wireless connection has roughly 5 times as much throughput as a 11 Mbps connection. However, the actual data transfer speed may be limited by other factors such as the Internet connection speed and other network traffic. Therefore, it is good to remember that the maximum throughput of a device or network may be significantly higher than the actual throughput achieved in everyday use.

TABLE 1: PARAMETER ANALYSIS OF EXISTING ALGORITHM

Number of nodes	PDR	E2E Delay	Throughput
10	66.6	0.563	7.57
20	59.67	0.557	28.29
30	45.12	0.560	36.16
40	42.71	0.595	66.13
50	38.21	0.579	81.70

TABLE 2: PARAMETER ANALYSIS OF PROPOSED ALGORITHM

Number of nodes	PDR	E2E Delay (ms)	Throughput
10	69.04	0.557	8.00
20	64.51	0.543	33.67
30	53.65	0.548	46.97
40	46.07	0.578	78.92
50	40.11	0.569	236.92

The results can also be compared graphically. The figure 1 to figure 3 shows the graphical comparison of the results. The figure 1 shows the comparison of PDR, 2 of E2Edelay and the 3 of throughput.

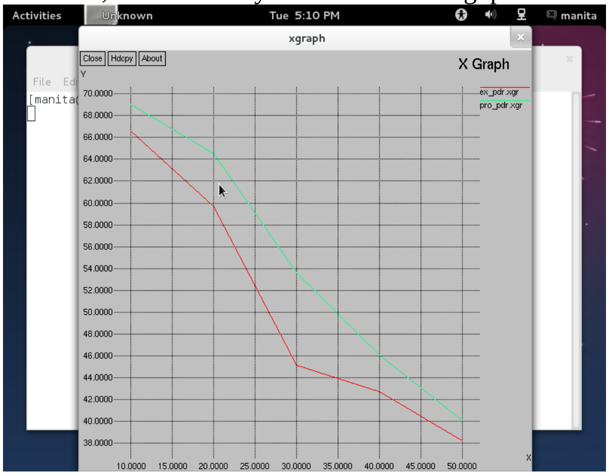

Figure 1: Comparison of PDR between the Existing And Proposed Algorithm

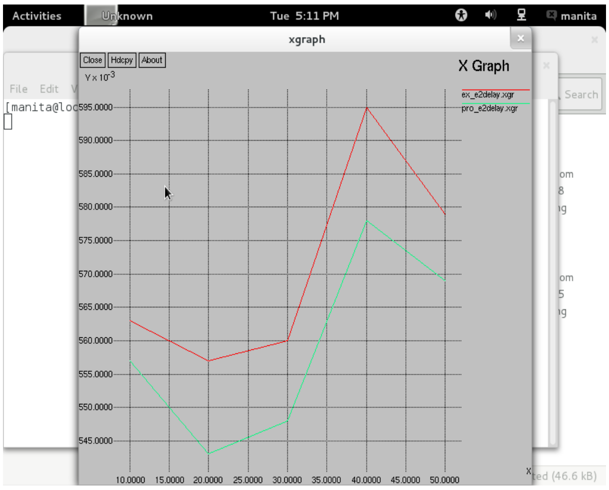

Figure 2: Comparison of E2E Delay between the Existing And Proposed Algorithm

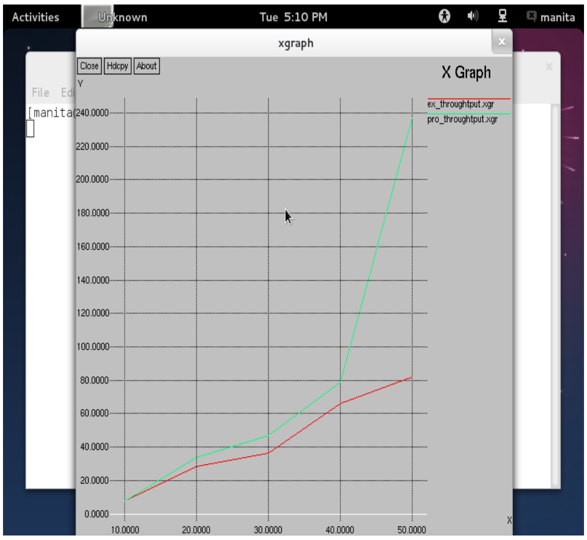

Figure 3: Comparison of Throughput between the Existing And Proposed Algorithm

The graphical comparison confirms the better performance of the proposed protocol is better than the existing protocol. The packet delivery ratio is increased and the delay get reduced and the throughput also get increased. It means overall performance get enhanced.

V. Conclusions

The security is more complicated in MANET when compared with ordinary network which the intruder may get physical access to the wired link or pass over security holes at firewalls and routers. Mobile adhoc network does not have a well-defined line of protection due to its infrastructure-free and each node shall be prepared for any threat. In wireless ad-hoc networks, the most important concern is routing issues. Actually, the old-fashioned techniques are not suitable in MANETs thus there is a need to modify current TCP/IP model to provide efficient functionality which has been made the routing protocols as key research area for investigators and challenging task as well. There are various routing protocols in MANET which are categorized in term of functionality as following: reactive protocols, proactive protocols and hybrid protocol.

This Paper modifies the AODV routing protocol by using ant colony optimization. This modified AODV detects the black hole as well as the gray hole attack and also recover from these attack. The simulation results confirm the better performance of the proposed protocol is better than the existing protocol. The packet delivery ratio is increased and the delay get reduced and the throughput is also get increased.

References

[1] Tseng, Fan-Hsun, Li-Der Chou, and Han-Chieh Chao. A survey of black hole attacks in wireless mobile ad hoc networks." Human-centric Computing and Information Sciences 1.1: 1-16.

[2] Swati Saini and VinodSaroha. 2013 Analysis and Detection of Black Hole Attack in MANET. International Journal of Science and Research. (May 2013).

[3] IztokFisterJr, “A Brief Review of Nature-Inspired Algorithms for Optimization”, [cs.NE] 16 Jul 2013.

[4] Oscar Cardon, Francisco and Thomas Stiitzle. A Review on the Ant Colony Optimization Metaheuristic: Basis, Models and New Trends. Mathware& Soft Computing 9 (2002)

[5] Lee, Seungjoon, Bohyung Han, and Minho Shin. "Robust routing in wireless ad hoc networks." In Parallel Processing Workshops, 2002. Proceedings. International Conference on, pp. 73-78. IEEE, 2002.

[6] Dokurer, Semih, Y. M. Erten, and Can ErkinAcar. "Performance analysis of ad-hoc networks under black hole attacks." In SoutheastCon, 2007. Proceedings. IEEE, pp. 148-153. IEEE, 2007.

[7] Jhaveri, Rutvij H., Sankita J. Patel, and Devesh C. Jinwala. "A novel approach for grayhole and blackhole attacks in mobile ad hoc networks." In Advanced Computing & Communication Technologies (ACCT), 2012 Second International Conference on, pp. 556-560. IEEE, 2012.

[8] Saetang, Watchara and SakunaCharoenpanyasak. "CAODV Free Blackhole Attack in Ad Hoc Networks." International Proceedings of Computer Science & Information Technology 35 (2012).

[9] CHuanhoQu, Lei Ju and ZhipingJia. “Light-weight Trust-based On-demand Multipath Routing Protocol for Mobile Ad Hoc Networks.”12th IEEE International Conference on Trust, Security and Privacy in Computing and Communications, 2013.