International Conference on Advancements in Engineering, Technology and Sciences
Dhaanish Ahmed College of Engineering, Chennai (ICAETS-2018)
(Approved by AICTE, New Delhi and Affiliated to Anna University, Chennai)
16th-17th March 2018 www.conferenceworld.in ISBN : 978-93-87793-11-8

Detecting Wormhole Attacks in Mobile Ad-Hoc Networks using Ant Colony Optimization

Mr.S.Sugumaran[1], Dr.P.Venkatesan[2]

[1]*Research Scholar/Dept. of ECE, SCSVMV University, Kanchipuram,(India)*

[2]*Associate Professor / Dept. of ECE, SCSVMV University, Kanchipuram,(India)*

ABSTRACT

Mobile Ad-hoc Network (MANET) is a Self Configuring Infrastructure less network and they not have any centralization unit. MANET routing protocol is very easy to construct in any environment and vulnerable due to various types of attack, route decision is not easy in the network. Wormhole attack is destroyed the security of the system and affecting the performance of the network. Route path selection is not sure to create the correct link between source to destination due to wormhole attack. In this work, Wormhole considered very seriously in the network. We proposed Ant colony Optimization (ACO) Technique in AODV routing protocol. AOC is identifying valued route and protected from wormhole. The simulation result is providing better routing decision against the Wormhole attacks.

Keywords: AODV, Wormhole, Ant Colony Optimization and Nodes

I.INTRODUCTION

A very attractive and promising category of wireless networks that has emerged is based on an Ad Hoc topology; these networks are called Wireless Ad Hoc Networks. The term wireless network implies a computer network in which the communication links are wireless. The term Ad Hoc comes from the fact that there is no fixed infrastructure for forwarding/ routing the packets. In Ad Hoc networks, each node is willing to forward data to other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. A MANET (Mobile Ad-hoc Network) is a one type of ad hoc network that has configuring itself continuously and it can change locations. The MANETS are portable, so they are using the wireless connections to connect the different networks.

Wormhole refers to an attack on MANET routing protocols in which colluding nodes create an illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbors but are actually distant from one another A wormhole attack is a particularly severe attack on MANET routing where two attackers, connected by a high-speed off-channel link, are strategically placed at different ends of a network. Viren Mahajan et. al., (2008) consider several terms for measuring the capacity of nodes involved in wormhole attack. S.Choi et. al., (2008) considered that all the nodes will monitor the behavior of its neighbors. Each node will send RREQ messages to destination. If source does not receive the RREP message within a define time, it detects the presence of wormhole and adds the route to its wormhole list. Yih-Chun Hu et.al., (2003) proposed Packet leash is a mechanism for detecting and thus defending against wormhole attacks. A leash is any

information on that is added to a packet designed to restrict the packets maximum allowed transmission distance.

Shalini Jain et al (2010) presented a novel trust-based scheme for identifying and isolating nodes that create a wormhole in the network without engaging any cryptographic means. With the help of extensive simulations, demonstrate that scheme functions effectively in the presence of malicious colluding nodes and does not impose any unnecessary conditions upon the network establishment and operation phase.

The Chiu et al. (2006) proposed the Hop Count delay per hop indication [DELPHI] method. Both the hop count and delay per hop indication (DELPHI) are monitored for wormhole detection here. The elementary assumption of this method is that, the rescheduling of a packet under normal condition for propagating one hop is very high in wormhole attack as the actual path between the nodes is longer than the advertised path.

Natt-Abdesselam et.al., (2008) proposed methodology for wormhole detection is also a two step process. In the first place, from a set of dislodge paths from sender to receiver, the route path information are collected. Each sender embraces a timestamp on a special DREQ packet and sigh it before sending it to the receiver. In this work, Ant Colony Optimization technique is proposed for detecting wormhole attacks on MANETs.

The Rest of the paper as followed, Section 2 – Discussed Literature review related to wormhole attack, Section-3 is Ant colony Optimization Algorithm. Section-4 simulation result and Discussion and Section-5 conclusion of the work.

II. WORMHOLE ATTACKS

It is a severe attack in ad hoc networks where two malicious nodes form a virtual channel among them [Anitha, P. and M. Sivaganesh, (2012), Eriksson, J., et al, (2006)]. Attackers pass the packet through virtual channel and replay them into the network. It can be launched even if the network communication uses cryptographic techniques. Wormhole may exists at bit level (the reply is done bit by bit even earlier than the whole packet arrived), same as cut through routing by [Wang. P., et al., (2014)] or at physical layer [Danev, B, 2012], [Eriksson, J., et al, (2006)]. In fact, nodes around the wormhole antenna realize that they can transmit packets with other wireless nodes located next to the other antenna and consider them as immediate neighbors. Lunching wormhole attack can be done easily. It is not depend on Medium Access Control (MAC) layer protocol and cryptography techniques are not enough to prevent it, as wormhole attackers do not create separate packets, but simply replay packets that already exist on the network by passing all cryptographic checks [Tellez, F. and J. Ortiz (2011)], [Keer, S. and A. Suryavanshi, (2010)]. It is due to the wormhole attacker no needs to break into wireless nodes or realize the mechanism of communication used by the network.

The packets can be transmitted over the wormhole link and reach to destination without any changes or dropping of any packets, the existence of wormhole is not harmful, and even have benefit by enhance the network connectivity and makes a shorter path to transfer packets between sender and receiver otherwise far off area. If the distance of tunnel is longer than transmission range, nodes near the wormhole antenna look for faster and shorter reliable paths by using the wormhole tunnel. Wireless networks running any dissimilarities of shortest path routing will find out this kind of paths and finally use them to broadcast data.

Wormhole attack turn off and on the signal replayed by the adversary and it completely changes the network

connectivity and then suddenly creates or destroys many of shortest paths in the network and upset most of routing protocols. Wormhole can get the RREQ packet through the tunnel and then play a denial of service attack by ignoring to broadcast any packets in on-demand routing protocols. In routing protocols which discover neighbors, the attacker can do frequent neighbor and path changes, it makes nodes consume the energy and wastes communication bandwidth. When the wormhole node is exist, it replay the scheme, mostly wormhole used to obtain network traffic, then spoof the packets, drop packets, or act as man in the middle attacks. In this way, when the traffic gathered, it helps to break encryption and security mechanisms of the network. Impact of wormhole attack is measured in terms of number of pairs whose shortest paths are affected.

Wormhole attacks have more impact, when two antennas are placed far apart, because of more paths and more traffic in the network; as a result, more damages are done to the transmitted packets by the wormhole link. In Figure 1 two red nodes N1 and N2 are wormhole and the dotted line connects two nodes is a long wormhole link. The blue nodes are normal nodes and they consist more hops to transmit packets to destination. When the attack happens, nodes located in area A consider nodes in area B as neighbors and vice versa. Overall, to messing up with the routing protocols, by using wormholes, adversary able to break any protocol relies on geographic proximity [Zhang, W., et al (2007)]. At the same time, every single one of localization algorithms which employ network connectivity would fail by the alteration of the network topology based on wormhole links. It can be the main impact of wormhole, due to its position which can be exploited as a useful function in numerous application as well as protocols. On the other hand, out of band location systems like Global Positioning System (GPS) cannot be accessible or unusable because of the environment [Dhurandher, S.K., et al. (2012)] [Keerthi, T.D.S. and P. Venkataram (2012)].

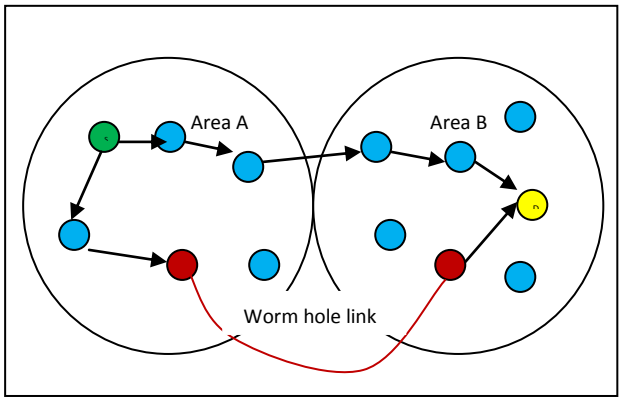

Figure 1 Demonstration of Wormhole Attack.

III. ANT COLONY OPTIMIZATION

Ant Colony Optimization (ACO) Nature-inspired meta-heuristics algorithms are flattering popular and powerful in solving optimization problems. Ant Colony Optimization is one of the finest algorithms for path finding. They develop their inspiration from the real-world behavior of ants and the method they use for finding food. ACO is based on the indirect communication of a colony of simple agents, called artificial ants, when an ant

moves along a path; it deposits a chemical called pheromone on it. As more and more ants move along the same path, the pheromone concentration of the path increases.

The path with the maximum pheromone concentration is then chosen to be the optimal path. A combinatorial optimization problem can be represented as a A = (x, y), where x is the solution space with x Є X a specific candidate solution and Y: X → R+ is a fitness function assigning positive values to candidate's solution. The goal of the algorithm is find a solution x*, or set of solutions X*, x* Є X* ⊆ X the increase the fitness function. Here, the x* is called optimal solution and X* is called the set of optimal solutions.

Algorithm for Ant Colony Optimization

Input: An instance I of a combinatorial problem p

1. Initialize Pheromone values (┌)
2. WHILE termination condition not met do
3. Schedule Activities
4. $S_i \leftarrow \rho$
5. For j=1,…….m_s do
6. $X \leftarrow Ant\ based\ solution\ Construction\ (\mu)$
7. X← $Local\ Search\ (X)$
8. $X_i = X_i\ U\ \{X\}$
9. End for
10. $Pheromone\ Updation\ (\Gamma)$
11. Daemon Actions ( ) {Optional}
12. END Schedule Activities
13. END WHILE
14. Output : Best solution found

The Features of ACO is a multi-agent organization, instant communication among the agents, distributed operations, and use of stochastic decision policy to construct solutions, instant learning of the parameters of the decision policy. In This work, ACO algorithm is basically interplay of three procedures: 1. Ant Based Solution Construction, 2. Pheromone Updating and 3. Daemon Actions, as represented by algorithm as given below. The schedule activities construct does not specify how these three activities are scheduled and synchronized. The designer is therefore free to specify the way these three procedures should interact. The Ant Based Solution Construction ( ) procedure performs probability of choosing the next sub solution of i, which is defined as follows:

$$\mu_{Sij} = \frac{\Gamma_{ij}^{p}(Q^q)}{\sum_{i \epsilon M_i^k} \Gamma_{ij}^{p}(Q^q)}; if\ j \epsilon M_i^k \quad (1)$$

Where M_i^K, is the set of Possible sub-solution that can be next sub-solution of i; Γij the pheromone value between the sub-solution of i and j; and Q_{ij} the quality of the subsolution j that will affect each ant's determination to move to j when at i. The parameter p and q are used to adjust the weight of exploration and exploitation. The Pheromone Updation () procedure is employed in updating the pheromone value Γij on each edge, which is defined as follows:

$$\Gamma^{ij} = (1 - \rho)\ \Gamma^{ij} \qquad (2)$$

Where ρ is the quality of solution created by ant, ρ € (0, 1) denotes the evaporation rate of pheromone value on the pheromone table. The Local Search () procedure is improving the quality of the solution of ACO.

IV. SIMULATION RESULTS AND DISCUSSION

The ultimate aim of the desertion is to implement a superior method to detect attacks in MANET. In this view, Wormhole attack in MANET is chosen. ACO methods are chosen for detecting the attack. The methods are implemented in AODV protocol and their performances are evaluated by the QoS such as Routing overhead and PDR. In this work, I have chosen the ns-2 simulator [ns] for this research includes an accurate model of the IEEE 802.11

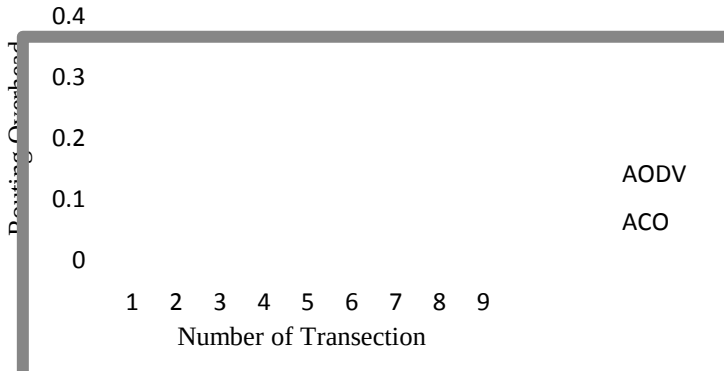

Figure 2 Number of Transactions Vs Routing Overhead for AODV and ACO.

because it realistically models arbitrary node mobility as well as physical radio propagation effects such as signal strength, interference, capture effect, and wireless propagation delay. The simulator also distributed the Coordination Function (DCF) in wireless MAC protocol. The DSDV routing protocol for wireless ad hoc networks is available within ns-2.

In AODV protocol if many nodes are sending and receiving data traffic simultaneously placing more malicious node uniformly causes severe

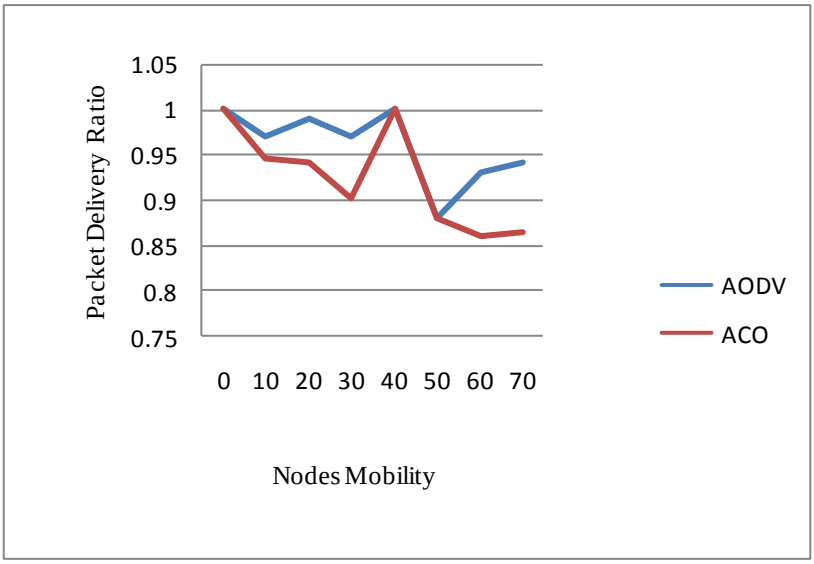

Figure 3 Nodes Mobility Vs Packet Delivery ratio for CSTR, CBR, NNT, AODV and ACO.

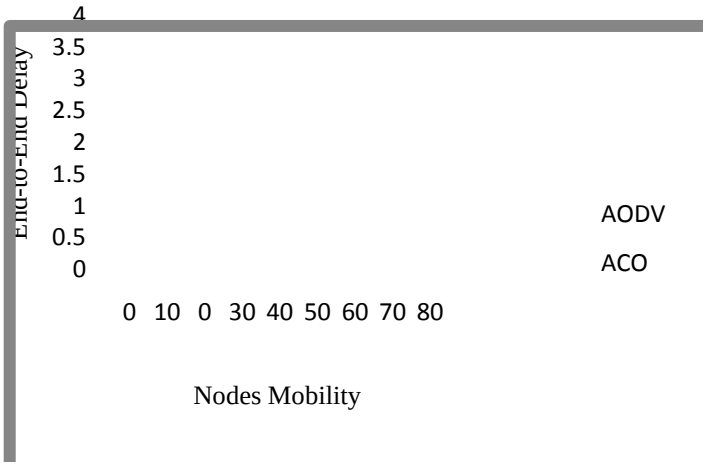

Figure 4 Nodes Mobility Vs End to End delay for AODV and ACO.

damage because it increases the probability of route affected malicious node. When there is number of malicious node packet delivery ratio is more, there is very less probability that any route involve malicious node and Packet Delivery Ratio decreases as the malicious node added to the scenario. From Figure 2,3,4 and 5, it is observed that ACO produces better results than other methods.

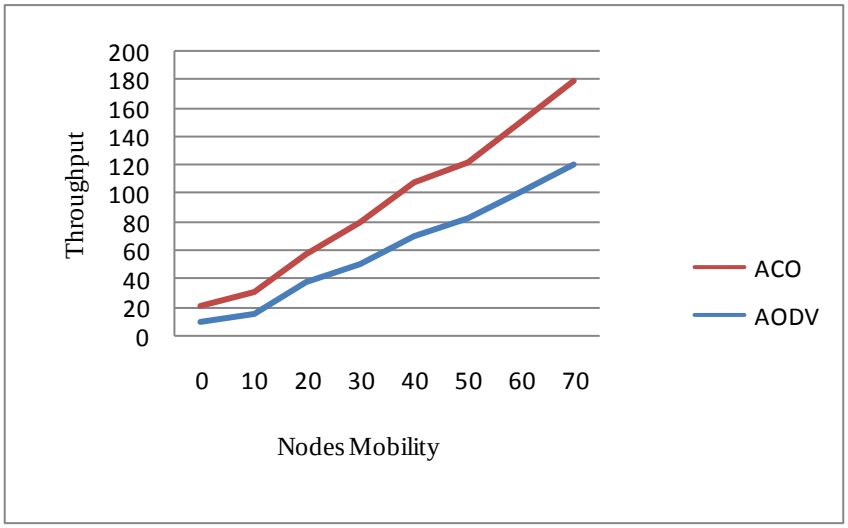

Figure 5 Nodes Mobility Vs Throughput for AODV and ACO.

V. CONCLUSION

In this work, results performed for detecting wormhole in MANET. ACO and AODV are considered for detecting wormhole attacks. Their performances are evaluated by Routing overhead, PDR, End to End delay and Throughput. Figure 2,3 4 and 5 shows the Routing overhead, PDR, End to End delay and Throughput for AODV and ACO by varying the number of nodes. From the responses, it is observed that the ACO outperforms other methods with respect to performance measures for all the scenarios. From the above figures, it is concluded that the ACO performs well as compare to AODV.

REFERENCES

[1]. Viren Mahajan, Maitreya Natu, and Adarshpal Sethi, Nov. 2008 "Analysis of wormhole Intrusion Attacks In MANETS",IEEE Military Communications Conference,MILCOM 2008.

[2]. S.Choi, D.Kim , D. Lee, J. Jung " WAP:Wormhole Attack Prevention Algorithm in Mobile Ad Hoc Network ", *In Proceeding International Conference on Sensor Networks, Ubiquitous and Trustworthy Computing*, 2008, pp. 343-348.

[3]. Yih-Chun Hu, Adrian Perrig, David B. Johnson, 2003 "Packet Leashes : A Defence against Wormhole Attacks in Wireless Networks", *Twenty-Second ANNUAL Joint Conference of IEEE Computer and Communications* , pp. 267-279.

[4]. Shalini Jain, Dr.Satbir Jain, " Detection and prevention of wormhole attack in mobile adhoc networks" , *In Proceedings of the International Journal of Computer Theory and Engineering, Vol. 2, No. 1* February, 2010, pp.78-86.

[5]. Chiu, HS; Wong Lui KS, 2006 "DELPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks",*In Proceeding of International Symposium on Wireless Pervasive Computing*, pp. 6-11.

[6]. F. Natt-Abdesselam, B. Bensaou, T. Taleb, "Detecting and Avoiding Wormhole Attacks in Wireless Ad Hoc Network", IEEE Communications Magazine, 46(4), pp. 127-133, 2008.

[7]. *Anitha,P and M.Sivaganesh,Detection and Prevention of Wormhole Attack in MANETS using Path Tracing.* International Journal of communications and networking systems, 2012. **1**(2).

[8]. Eriksson, J., S.V. Krishnamurthy, and M. Faloutsos. *Truelink: A practical countermeasure to the wormhole attack in wireless networks*. in *Network Protocols, 2006. ICNP'06. Proceedings of the 2006 14th IEEE International Conference on*. 2006. IEEE.

[9]. Wang, P., et al., *A Comprehensive Comparison between Virtual Cut-through and Wormhole Routers for Cache Coherent Network On-chips.* IEICE Electronics Express, 2014. **11**(14).

[10]. Danev, B., D. Zanetti, and S. Capkun, *On physical-layer identification of wireless devices.* ACM Computing Surveys (CSUR), 2012. **45**(1): p. 6.

[11]. Tellez, F. and J. Ortiz, *Behaviour of Elliptic Curve Cryptosystems for the Wormhole Intrusion in Manet: A Survey and Analysis.* IJCSNS International Journal of Computer Science and Network Security, 2011. **11**(9): p. 1-12.

[12]. Keer, S. and A. Suryavanshi. *To prevent wormhole attacks using wireless protocol in MANET*. in *Computer and Communication Technology (ICCCT), 2010 International Conference on*. 2010. IEEE.

[13]. Zhang, W., et al., *Security issues in wireless mesh networks*, in *Wireless Mesh Networks*. 2007, Springer. p. 309-330.

[14]. Dhurandher, S.K., et al. *E2siw: An energy efficient scheme immune to wormhole attacks in wireless ad hoc networks*. in *Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on*. 2012. IEEE.

[15]. Keerthi, T.D.S. and P. Venkataram. *Locating the attacker of wormhole attack by using the honeypot*. in *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on*. 2012. IEEE.