Current Trends in Technology and Science
ISSN: 2279-0535. Volume: 6, Issue: 1

Multipath Reliable Ant Optimized Secure and Congestion Free Communication under MANET

Shanti Rathore
Lecturer Dept. of electronics and telecommunication Govt. polytechnic janjgir champa Janjgir, chhatisgarh
rathoreshanti@gmail.com

Dr. M. R. Khan
HOD Dept. of electronics and communication
Principal of government Engineering Collage
Jagdalpur, chhatisgarh
mrkhan@gecjdp.ac.in

Abstract—in this research we proposed the security in ANT Optimized based multipath congestion routing performance. The scenario of DDoS is simulated and examines their effect in dynamic network. The multipath protocol like AOMDV is balance the load by providing alternative path but not proficient at every condition. The DDoS attacker is blocking the entire possible path in network by flooding huge amount of redundant packets in dynamic network. The attacker is the intermediate node and this attacker infection is continuously dispersing infection and the entire network performance is dumped. The proposed security scheme is identified attacker and their loss effect. Attacker is fully disabled by proposed security mechanism and their loss is also evaluated. The proposed method is not only detecting but also prevent network from DDoS attack. The performance of security scheme and attack is measured in three different scenarios of different node densities. The proposed scheme is provides attacker free routing and recover network performance after applying it. The performance of ANT OPTIMIZED and security is almost equal. The packets receiving, throughput, and PDR are enhancing but the loss of packets and unnecessary flooding is reduced in dynamic network.

Keyword: - *MANET, AOMDV, ANT optimized, DDoS, Security, Routing.*

I. INTRODUCTION

A Mobile Ad hoc Network is a collection of mobile nodes forming an ad-hoc network without the assistance of any centralized structures. These networks introduced a new art of network establishment and can be well suited for an environment where either the infrastructure is lost or where deploy an infrastructure is not very cost effective. The popular IEEE 802.11 "WI-FI" protocol is capable of providing ad-hoc network facilities at low level, when no access point is available. However in this case, the nodes are limited to send and receive information but do not route anything across the network. Mobile ad-hoc networks can operate in a standalone fashion or could possibly be connected to a larger network such as the Internet [1].

Mobile Ad hoc Networks [2, 3] can turn the dream of getting connected "anywhere and at any time" into reality. Typical application examples include a disaster recovery or a military operation. Not bound to specific situations, these networks may equally show better performance in other places. As an example, we can imagine a group of peoples with laptops, in a business meeting at a place where no network services is present. They can easily network their machines by forming an ad-hoc network. This is one of the many examples where these networks may possibly be used.

Ad hoc On-Demand Multipath Distance Vector (AOMDV) shares numerous characteristics with AODV [3]. It is based on the distance vector routing and uses hop-by-hop routing approach. Furthermore, AOMDV also finds routes on demand using a procedure of route discovery. The main difference is in the number of routes found in each route discovery. In AOMDV, route request (RREQ) transmission from the source towards the destination establishes multiple reverse paths both at intermediate nodes as well as the destination. Multiple route reply (RREPs) traverse these reverse paths back to form multiple forward paths to the destination at the source and intermediate nodes. Note that AOMDV also provides intermediate nodes with alternate paths as they are found to be useful in reducing route discovery frequency [4]. AOMDV relies on the routing information already available in the underlying AODV algorithm, thereby limiting the overhead incurred in discovering multiple paths. It does not employ any special control packets. In reality, extra RREPs and RERRs for multipath discovery and maintenance along with a few extra fields in routing control packets (i.e., RREQs, RREPs, and RERRs) constitute the only additional overhead in AOMDV relative to AODV.

II. CONGESTION AVOIDANCE

During the initial data transfer phase of a TCP connection [5] the Slow Start algorithm is used. However, there may be a point during Slow Start that the network is forced to drop one or more packets due to overload or congestion. If this happens, Congestion Avoidance [6] is used to slow the transmission rate. However, Slow Start is used in conjunction with Congestion Avoidance as the means to get the data transfer going again so it doesn't slow down and stay slow. In the Congestion Avoidance algorithm a retransmission timer expiring or the reception of duplicate ACKs can implicitly signal the sender that a network congestion situation is occurring. The sender immediately sets its transmission window to one half of the current window size (the minimum of the congestion window and the receiver's advertised window size), but to at least two segments. If congestion was indicated by a timeout, the congestion window is reset to one segment, which automatically puts the sender into Slow Start mode. If congestion was indicated by duplicate ACKs, the Fast Retransmit and Fast Recovery algorithms are invoked (see below). As data is received during Congestion Avoidance, the congestion window is increased. However, Slow Start is only used up to the halfway point where congestion originally occurred. This halfway point was recorded earlier as the new transmission window. After this halfway point, the congestion window is increased by one segment for all segments in the transmission window that are acknowledged. This mechanism will force the sender to more slowly grow its transmission rate, as it will approach the point where congestion had previously been detected.

III. ANTCOLONY OPTIMIZATION IN ROUTING

ACO routing algorithms take inspiration from the behavior of ants in nature and from the related field of ACO to solve the problem of routing in communication networks. The main source of inspiration is found in the ability of certain types of ants (e.g. the family of Argentine ants Linepithema Humile) to find the shortest path between their nest and a food source using a volatile chemical substance called pheromone. Ants traveling between the food source and the nest leave traces of pheromone as they move. They also preferentially go in the direction of high pheromone intensities. Since shorter paths can be completed faster, they receive higher levels of pheromone earlier, attracting more ants, which in turn lead to more pheromone. This positive reinforcement process allows the colony as a whole to converge on the shortest path. This forms the basis of most of the work in the field of ACO [7].

IV. PREVIOUS WORK ACCOMPLISHED

The previous work in field of ACO, Congestion and DDoS is proposed by various researches and this work is present in this section.

Mohammad Golshahi, Mohammad Mosleh, Mohammad Kheyrandish The authors of [8] Introduces a multi path hybrid routing algorithm for mobile Ad-hoc networks. This algorithm is based on swarm intelligence algorithms and Ant Colony Optimization (ACO), particularly. By mapping arithmetic and engineering problems on to biological societies, these methods attempt to solve the problems. In the presented algorithm, the number of neighbors of a node has been used to select the next hop.

S. Kannan , T. Kalaikumaran , S. Karthik and V.P. Arunachalam In [9], the authors Propose EAQR, a novel routing protocol based on an improved Ant colony optimization (ACO) algorithm. The algorithm concentrates on the provision of QoS and balanced energy-consumption over the whole network. With the introduction of some metrics like the minimum path energy and path hop count and by means of advancing pheromone trail model of the ant colony system, the algorithm innovatively provides two heuristic ways respectively based on the length and the comfort of path to meet the different performance requirements of real time and common traffics. ACO-AOMDV is presented in

Xun-bing Wang, Yong-zhao Zhan, Liang-min Wang, Li-ping Jiang [10]. The authors presents an ant colony optimization and ad-hoc on-demand multipath distance vector (AOMDV) based routing protocol (ACOAOMDV) for ad hoc networks. In ACO-AOMDV, ant packets deposit simulated pheromone as a function of multiple parameters corresponding to the information collected each path visited, such as average link count of path, average load of path, hop count and the current pheromone the nodes possess and so on, and provide the information to the visiting nodes to update their pheromone tables by endowing the above different parameters corresponding to different information with different weight values.

Rajeshwar Singh, D K Singh, Lalan Kumar,In [11], a hybrid QoS routing algorithm which can improve the performance in MANET is proposed. The hybrid quality of the algorithm makes it suitable for all the environments in comparison with reactive and proactive protocols. Ant's pheromone update process approach has inherited advantage of robustness and fast convergence, which makes it an appropriate choice over existing QoS algorithms to improve the performance for MANET.

Eseosa Osagie, Parimala Thulasiraman and Ruppa K. Thulasiram The authors of [12] Develop an improved routing algorithm for MANETs based on Ant Colony Optimization (ACO) inspired by real ants. The performance of the routing algorithm is evaluated through simulation and is compared to an existing well known MANET routing protocol, Ad hoc On-Demand Distance Vector (AODV). Several performance metrics are considered in different scenarios with varying mobility levels and traffic load.

V. PROPOSED SECURE ROUTING

Mobile ad-hoc network are form through collection of nodes whose work like agent in between sender to receiver. Through the related research papers we find out the research problem and optimized it. In this paper we design an optimal protocol that enhanced the security features of MANET and provide congestion free communication under different circumstances or structure. Proposed security and congestion control mechanism inherited through AOMDV and Ant colony optimization mechanism, because these techniques helps to find out best suitable multiple path from source to destination and provide reliable communication. ad-hoc on demand multipath distance vector routing useful while more than one path are needed for the communication, its provide load balancing facility to the entire network that prefer three best shortest path out of all available paths but it's not suitable for all pair of communication so in our proposed approach we tune or optimized multipath selection through Ant colony optimization (ACO) methodology.

DDOS Prevention:

Distributed denial of service attack are change the network behaviour due to network node abnormal functionality so DDOS attack is generate multiple misleading behaviour of network i.e. routing, data formatting, spoofing etc. our proposed Ant base security mechanism provide lightweight security method and more suitable for dynamic network, because we tune the network through its pheromone behaviour, the nodes pheromone is useful to detection of DDOS nodes so in future can't enter the junk message generated by DDOS attacker within the network and minimized the congestive environment. DDOS attacker node spread the junk message to the vulnerable node using handshake method and captures it, that message forward to next hop and after short period of time whole network is crash.

Algorithm 3: DDOS Detection and Prevention

Input:

M: mobile nodes
S: sender nodes
R: receiver nodes
I: Intermediate nodes
Ψ= radio range
AOMDV: routing
S_i: Suspicious nodes
A: Attacker nodes
P: Preventer nodes

O: Optimization technique (ACO)
f_z = {0.0,0.1,0.2,……..1.0}

$$PH = \prod_{p=0}^{1} h_p{}_0 h_p \text{ Pheromone value}$$

Output: TCP, UDP, attacker Percentage, Attacker node identification

Procedure:

AOMDV(S, R, route_pkt, Ψ)
If (I in Ψ and I != R) **then**
I← set ph (0 to 1) forwarding criteria
I← forward route_pkt
Else if (I== R && path> 1) **then**
Select best three paths whose ph value higher
Send acknowledge to S using reverse path
Data(S, R, I)
Else
Node out of range or not receiver reachable
End if

DDOS detection/prevention

P watch I nodes
If (I send junk message && m_1 receives) **then**
m_1 ← congested
m_1 ← not forward genuine pkt
m_1← broadcast junk message to M
capture all M nodes
network congested
Else
Network forward date through normal paths
Use ACO by all M nodes
Calculate new_ph of I nodes ← (forward / receives) ± old_ph
Classify I node by f_z value
Update route through new_ph value
End if

P execute detection module
If (I send junk message && pkt! = normal) **then**
Set I as S_i
S_i ← receives && not forward
A← S_i
Detect by P packet type of A,
Time of attack
Node number
Number of junk message

End if

P execute prevention module
If node detect junk spreader && A ← DDOS **then**
A_{ph} ← 0
P← broadcast node A as attacker
P← block A node
End if

VI. Simulation Parameter

The simulation of previous and proposed protocol is simulated on the basis of these considered parameters. These parameters are common in DDoS attacker presence and security scenario.

Table1 Simulation Parameters

Parameters	Type
Network Type	MANET
Mobile Nodes	10, 30, 50
Physical Medium	Wireless Physical
Propagation Modes	Two Ray Ground
Antenna Type	Omni Directional Antenna
Simulation Area	800*800 m2
Simulation Time	100 seconds
Frequency	914e+6 Mhz
MAC Layer	802.11
Routing Protocol	AOMDV, ANT
Attack Type	DDOS
Prevention	Message identification
Queue Type	Drop tail/ Priority Queue

VII. Results and Discussion

The results evaluation and discussion is mentioned in this section that measures the performance in presence of DDoS attack and security.

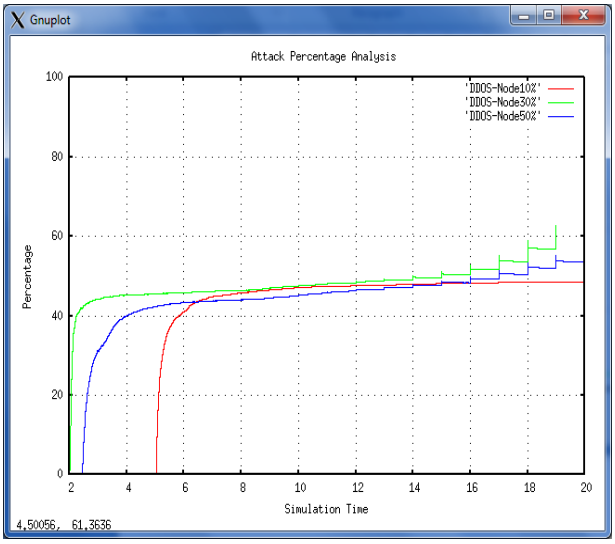

Fig.1 Attacker Loss Analysis

A. Attacker Percentage Analysis

The DDoS attacker in network is flooding unwanted packets and these packets are degrades network performance by blocking link capacity. The attacker nodes are also infected other nodes that perform same activities in network as attacker. In this graph the drop due to attacker presence is measured in all three scenarios of different node density. The data dropping in different node density is different but the proposed security scheme is prevent network from malicious effect of attacker and provides secure routing. The attacker infection is increase with respect to time and maximum drop percentage is reaches 60 %. The attacker drop percentage is completely removes from network after applying security scheme in dynamic network.

B. Attack Detection in 10 nodes Scenario

The DDoS attacker is flooded unwanted packets in network and these packets are not contain any useful data because of that these packets are only flooded in network for consuming limited bandwidth capacity. In DDoS attacker is spread their malicious behaviour and due to attacker infection other nodes are also behaves like

attacker. In this table 1, table 2 and table 3 the different scenario of node density is mention and identified that the number of attacker quantity is different in different node density scenario. In 10 node density only node 4 is not flooded large amount and their infection is also minimum. In scenario of 30 nodes and 50 node huge amounts of packets are flooded by many nodes. In 10 nodes scenario number of attacker are 6 nodes, in 30 nodes scenario number of attacker are 8 nodes and in 50 mobile nodes scenario number of attacker are 7 nodes in dynamic network.

Table 1 Attacker Analysis in 10 node density

DDOS Attacker	Packet Spread	Percentage of Infection
2	59828	11.26
3	50410	9.49
4	589	0.11
5	47945	9.02
6	55481	10.44
7	43843	8.25

Table 2 Attacker Analysis in 30 nodes densit

DDOS Attacker	Packet Spread	Percentage of Infection
8	67850	6.21
9	43567	3.99
12	185710	17.01
15	43904	4.02
17	55517	5.08
20	41416	3.79
21	67614	6.19
29	178515	16.35

Table 3 Attacker Loss in 50 nodes Density

DDOS Attacker	Packet Spread	Percentage of Infection
2	45218	6.06
7	66841	8.95
24	39303	5.26
27	128547	17.21
32	42770	5.73
34	6404	0.86
36	70138	9.39

VIII. Conclusion and Future Work

The possibility of attacker existence is more if the flooding of packets are uncontrolled and incessantly increases with respect to time. The proposed security scheme is applied on ACO (Ant Colony Optimization) pheromone based multipath to secure network from the DDoS attack. The attacker is detected by the heavy flooding of routing packets and these packets flooded by the node are addressed by security scheme to block it permanently in network. The effect of proposed scheme is that the processing capability of nodes are utilized for maximum data forwarding to next neighbor and receiving proper response from neighbor or sender. The proposed scheme is much better to secure network from harmful DDoS attacker. The performance of network is measure in three different node density scenario and results are obviously shows the strong affect of proposed scheme by enhancing packets receiving and removes flooding effect of attacker. The presence of proposed security mechanism is reducing packets loss and flooding and improves throughput and PDR performance in dynamic network.

In future we also measure the some extra performance analysis of proposed security scheme in transport layer protocol. The TCP and UDP are the transport layer protocol and their performance in term of packet loss is measures.

References

[1] Tasman Networks Inc. Routing basics: Protocol evolution in enterprise and service provider networks. Technical report, 2004.

[2] Yang H., Luo H., Ye F., Lu S., Zhang L. "Security in Mobile Ad Hoc Networks: Challenges and Solutions", IEEE Wireless Communications, Vol. 11, No. 1, pp. 38 -47, 2004.

[3] Mahesh K. Marina, Samir R. Das, "Ad hoc On-Demand Multipath Distance Vector Routing", Wireless Communications And Mobile Computing, Published online in Wiley Inter Science (www.interscience.wiley.com), 6:969–988, 2006.

[4] A Nasipuri, R Castaneda, SR Das SR, "Performance of multipath routing for on-demand protocols in mobile ad hoc networks". ACM/Kluwer Mobile Networks and Applications (MONET), 6(4):339–349, 2001.

[5] Jingyuan Wang, Jiangtao Wen et. al. in his work titled "An Improved TCP Congestion Control Algorithm and its Performance" 2011 IEEE.

[6] Makoto Ikeda, Elis Kulla, Masahiro Hiyama, Leonard Barolli, Rozeta Miho and Makoto Takizawa "Congestion Control for Mul i-flow Traffic in Wireless Mobile Ad-hoc Networks", IEEE Sixth International Conference on Complex, Intelligent, and Software Intensive Systems, 2012.

[7] M. Subha,Dr. R. Anitha, "An Emerging Ant Colony Optimization Routing Algorithm (Acora) For MANETs, Journal of Computer Applications", Vol-II, No.3, July-Sep 2009.

[8] Mohammad Golshahi, Mohammad Mosleh, Mohammad Kheyrandish," Implementing an ACO Routing Algorithm for ADHOC Networks," Proceeding of the IEEE International Conference on Advanced Computer Theory and Engineering, 2008

[9] S. Kannan , T. Kalaikumaran , S. Karthik and V.P. Arunachalam, "Ant Colony Optimization for Routing in Mobile Ad-Hoc Networks," International Journal of Soft Computing, Vol. (5), Issue (6), pp. 223-228, 2010.

[10] Xun-bing Wang, Yong-zhao Zhan, Liang-min Wang, Li-ping Jiang, "Ant Colony Optimization and Ad-hoc On-demand Multipath Distance Vector (AOMDV) Based Routing Protocol," Proceedings of the Fourth International Conference on Natural Computation, 2008.

[11] Rajeshwar Singh, D K Singh, Lalan Kumar, "Ants Pheromone for Quality of Service Provisioning In Mobile Ad-hoc Networks," International Journal of Electronic Engineering Research, Vol. (2), No. (1), pp. 101–109, 2010.

[12] Eseosa Osagie, Parimala Thulasiraman and Ruppa K. Thulasiram, "PACONET: imProved Ant Colony Optimization routing algorithm for mobile ad hoc NETworks, " IEEE Computer Society 22nd International Conference on Advanced Information Networking and Applications, pp. 204-2111, 2008.