ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 3, March 2014

Analysis of Attacks in Manet with Secure and Non- Secure Routing Protocols

Pertreesia Maria.T[1], Aranganathan.A [2]

M.E Student, Dept of ETCE, Sathyabama University, Chennai, India [1]

Asst. Professor, Dept of ETCE, Sathyabama University, Chennai, India [2]

ABSTRACT: Mobile Ad-hoc Networks is a multi-hop based wireless network consists of a set of mobile nodes that can communicate each other. Mobile Adhoc Networks have several vulnerabilities to network attacks. The performance analysis of the secure and non-secure routing protocol along with the attacks in the network layer is done. The non-secure routing protocol considered in this paper is ODMRP and the secure routing protocol is proposed by adding, additional features to the existing ODMRP. The additional feature includes the inclusion of the cryptographic method and the mobile agents. The cryptographic scheme employs PKI and the mobile agents are ANTS. The mobile agent employs ARA. A comparison is done between these protocols in terms of bandwidth, packet delivery ratio and multicast forwarding overhead and is observed that the secure protocol provides considerable enhancements. This is implemented by using ns-2 tool.

KEYWORDS: MANET, ODMRP, PKI, ARA, NS-2.

I. INTRODUCTION

A mobile ad hoc network is a self – organizing system of mobile nodes that communicate with each other via wireless links with no infrastructure or centralized administration such as base stations or access points. Each nodes in a MANET operates both as hosts as well as routers to forward packets. Finds application in an infrastructure-less operation such as emergency rescue and mining operations.

In these applications, communication and collaboration among a given group of nodes are necessary. In the place of using multiple unicast transmissions, it is advantageous to use multicast routing to save network bandwidth and related resources, since a single message can be delivered to multiple receivers simultaneously. Multicast routing protocols has two classifications: tree based and mesh based. In a multicast routing tree, there is usually only one single path between a sender and a receiver, while in routing mesh, there may be multiple paths between sender – receiver. Typical mesh based multicast routing protocols are ODMRP, CAMP, etc.

Among all the research issues, security is an essential requirement in ad hoc networks. Compared to wired networks, MANETS are more vulnerable to security attacks due to the lack of a trusted centralized authority. The security issue of MANETS in group communication is even more challenging because of multiple senders and multiple receivers. Several types of security attack in MANETS have been studied in the literature, and the focus of earlier research is on unicast applications. The effects of security attacks on multicast in ad hoc networks have not yet been solved. In this paper, we present simulation-based study which presents the performance of the newly proposed method along with the inclusion of attacks that exists in the network layer

II. RELATED WORK

In [1], the paper proposed a new destination driven multicast routing protocol which improves the multicasting efficiency. D-ODMRP enhances an existing multicast routing protocol ODMRP by introducing a destination driven strategy. The results showed that DODMRP can significantly improve the forwarding efficiency as compared with ODMRP with little extra protocol overhead. The destination-driven strategy is simple and efficient, and can also be introduced into other existing multicast routing protocols.

In [2], [3], the idea of swarm intelligence and the ants along with the security is proposed. [2]The swarm intelligence (SI) routing inspires from insect communities such as bees and ants to find and optimizes routes within an ad hoc networks. All the existing implementations of swarm routing does not give any consideration to security, which is a persistent requirement for wireless network so to improve the security ,the Public key infrastructure had been introduced(PKI). The proposed scheme called ANTPKI gave an implementation of PKI which is thoroughly independent from the underlying SI routing protocols and it almost ensures to include all the security services by taking advantages of the nature of the underlying routing protocol. It guarantees data confidentiality by means of session key establishment and at the same moment of the certificate publishing and using the same requests. [3] The protocol is based on swarm intelligence and on the ant colony optimization. This paper shows how an ant functions and how efficiently it can be employed for the purpose of reducing the overhead in an adhoc network.

In [4],[5] the paper defines how the MA[4] have been employed for the efficient reservation of bandwidth as inefficient resource allocation leads to improper functioning of the network.[5] defines various attacks that exists in an network layer of the protocol stack and how hardly it can affect the performance of an network leading it malfunction. In [6], the performance of a multicast session in a MANET under attack depends heavily on many factors such as the number of multicast receivers; the number of multicast sender's .The study of multicast routing along with the attacks is done and is compared with other routing protocol which is observed as comparison in terms of different performance metrics.

III. EXISTING WORK

1) ATTACKS IN MANET:

The two major attacks that exist in the MANET are considered here:

Wormhole attack: In a wormhole attack, two attacker nodes join together. One attacker node receives packets at one point and "tunnels" them to another attacker node via a private network connection, and then replays them into the network. Wormhole attack is a relay-based attack that can disrupt the routing protocol and therefore disrupt or breakdown a network and due to this reason this attack is serious. We can use following steps to explain about a general wormhole attack. An attacker has two trusted nodes in two different locations of a network with a direct link between the nodes. The attacker records packets at one location of a network. The attacker then tunnels the recorded packets to a different location. The attacker re-transmits those packets back into the network location.

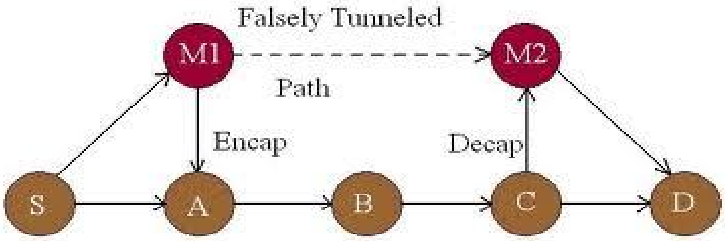

Fig 1: wormhole attack

Black hole Attack*:* In this type of attacks, malicious node claims having an optimum route to the node whose packets it wants to intercept. The malicious node sends a fake reply with extremely short route when it receives the route request .The node places itself between the communicating nodes, and does anything with the packets passing between them. For example, in figure, malicious node "c" advertises itself in such a way that it has a shortest route to the destination. The route discovery process is initiated and the source S forwards the data to the destination D. The malicious node "c" when receives the route request, it immediately sends response to source.

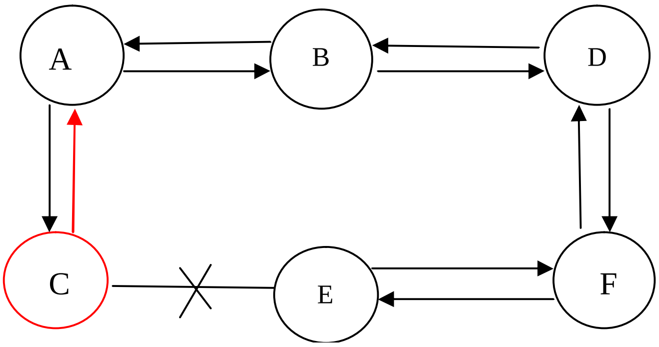

Fig 2: black hole attack

If reply from node "c" reaches first to the source than the source node "S" ignores all other reply messages and begin to send packet via route node. As a result, all data packets are consumed or lost at malicious node.

2) ROUTING PROTOCOLS:

The on demand multicast routing protocol (ODMRP) is a mesh based multicast routing protocol. It establishes a multiple path between the source and receiver. It uses the forwarding group concept for routing purpose. The functioning is that the sender floods the route with the join query packet. A routing table is maintained for maintaining the backward learning and for doing rebroadcasting. The receiving node on receiving the request generates the join reply and it checks for the next node id. On matching, the forwarding group is generated and through which the packets are propagated via the shortest path.

The destination driven on demand multicast routing protocol (DODMRP) incorporates the destination driven strategy. It includes the deferring time into the network. It achieves high multicast forwarding efficiency in the routing process. The processing is that it reduces the extra cost while selecting the routes though multiple paths exists it chooses the path with least extra cost.

IV. PROPOSED WORK

The proposed work aims in providing a secured routing protocol which functions even if the network layer attack exists and which also employs Ant as a mobile agent and PKI system for providing the overall security in the multicast routing protocol. The protocol considered is, MASODMRP (Mobile Agent secure-ODMRP).

1) ARA-ANT ROUTING ALGORITHM:

The Ant Routing Algorithm ARA uses artificial ants and pheromone to discover and optimize route from a given source node S to a destination node D in a MANET. Generally, ARA uses two kinds of artificial ants for route discovery and establishment.

The first one is called forward ant (FANT), which is used to discover routes from the source to the destination node. Therefore this ant travels over the entire network in order to find any possible route from S to D, similar to the discoverer ants in real ant colony which go far in the nature in order to find any possible source of food, during her trip over the network each ant deposits a constant amount of artificial pheromone used after by the intermediate nodes to shorten paths. The second category are the ants called backward ants (BANT), they follow the same path established by the FANTs and establishes the final route from S to D. Therefore the BANT travels over the same path discovered by the corresponding FANT from D to S in order to inform S about all the possible routes.

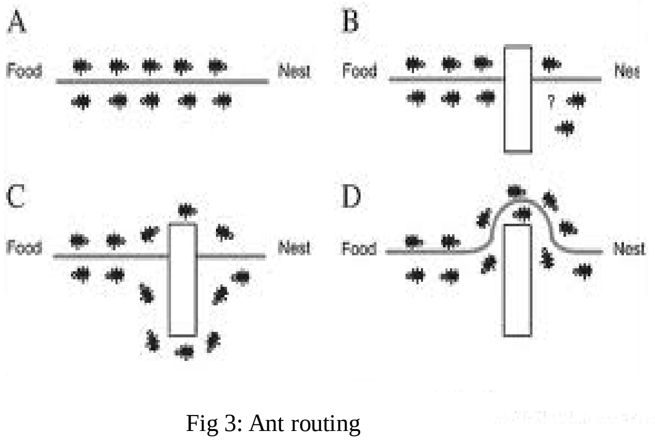

Fig 3: Ant routing

2) ANT-PKI

The ARA does not provide the efficient security though it possesses excellent routing capability. Thus for the purpose of providing security PKI is employed. In Ant PKI the certificate are self-issued by each node in the network, hence each node is responsible of the information contained in its certificate as well we suppose that each node have the capability of generating and keeping in secret its certificate, private and public key. when any node joins the network for the first time it must generate a certificate and fills it with the adequate information such as the user name, validity period, public key, MAC and IP address, signs this certificate with its private key, and waits for the appropriate moment to publish the certificate for the rest of nodes. It gives two services certificate publishing and certificate revocation. The structure of the forward ant is changed by creating new fields, the first one is used by the source node in order to publish its certificate for the rest of nodes and the second one is used by intermediate nodes to publish their certificate for their neighbours.

INTERMEDIATE NODE CERTIFICATE	SOURCE NODE CERTIFICATE	ORIGINAL FANT

Fig 4: structure of fant

DESTINATION NODE CERTIFICATE	SESSION KEY	ORIGINAL BANT

Fig 5: Structure of bant

In order to ensure security, we employ asymmetric crypto system i.e. digital signatures. They employ a private key to encrypt the data at the sender send, and the receiver can decrypt it by using the sender's public key. When this is employed in the process of data forwarding in MANET, even an attacker cannot attack or hack the data. And thus, by this means the security can be achieved.

V. SIMULATION RESULTS

The simulation results shows the performance between the existing and the proposed protocol .The proposed method with the results shown below

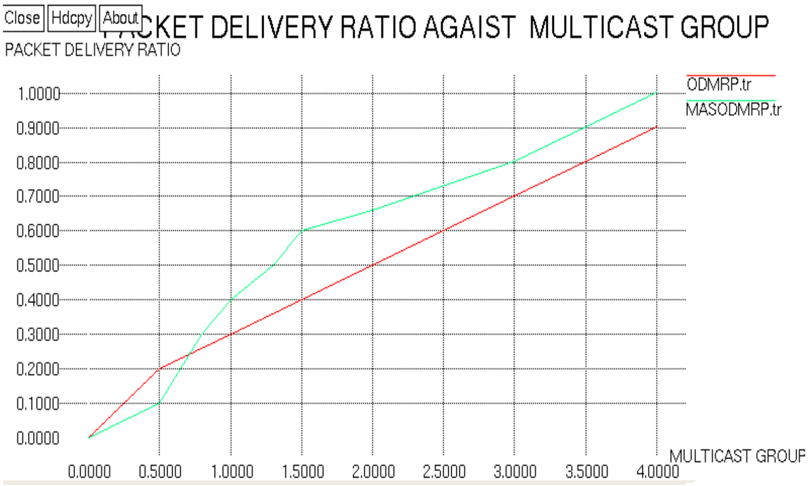

Fig 6: PDR

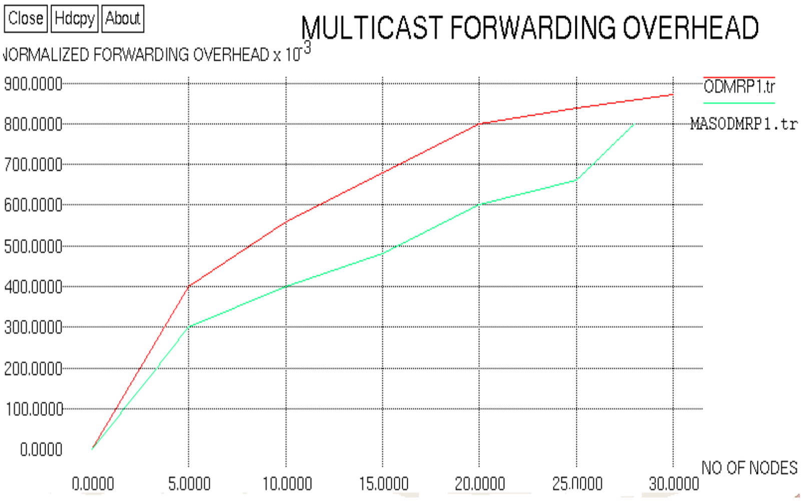

Fig 7: Multicast forwarding overhead

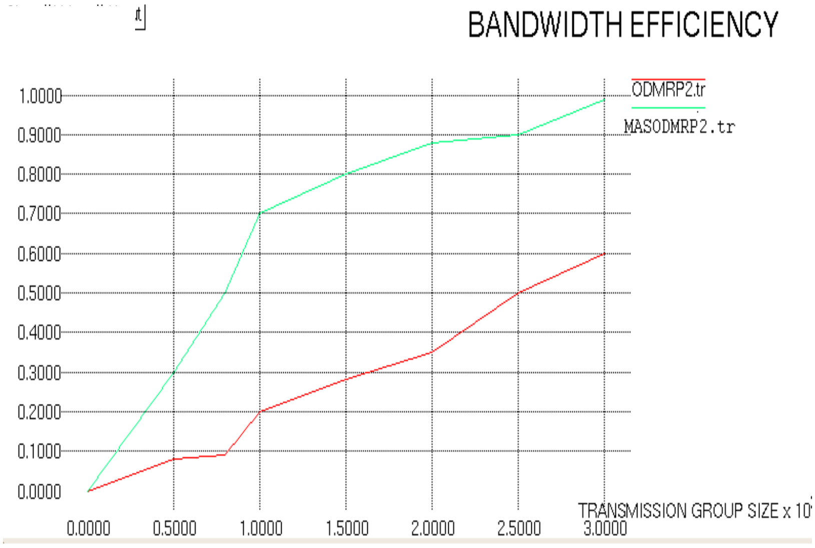

Fig 8: Bandwidth efficiency

Table 1: simulation Parameters

Simulation parameters	Black hole/wormhole
Channel type	Wireless
Radio-propagation model	Two ray ground
Ne	Wireless physical
M/	802.11
Interface queue type	Queue/drop trail/priqueue
Link layer type	LL
Antenna model	Omni antenna
Max. packet in ifq	50
Number of mobile nodes	28
Routing protocol	Masodmrp
X dimension of topography	3000
Y dimension of topography	3000
Time of simulation end	10.0
Number of malicious node	2

VI. CONCLUSION

This paper has designed a secured routing protocol which employs ant as a mobile agent and PKI security system for the purpose of analysing the network layer attacks and is aimed to reduce the multicast forwarding overhead which is the main problem that has to be considered while using multicast routing protocol. And the others parameters such as Bandwidth and Packet delivery ratio has also been accounted and the simulation results show that considerable improvement is achieved in the proposed work. The future work can be done with other multicast routing protocols which include other layer attacks to improve the network performance with the combination of digital signature and hash algorithm.

REFERENCES

[1] Y. Yan , K. Tian , K. Huang ,B. Zhang ,J. Zheng , “D-ODMRP: A destination-driven on-demand multicast routing protocol for mobile adhoc networks” IET communications. ISSN 1751-8628. 2012

[2] B.D. Shirodkar , S.S Manvi , A.J.Umbarkar " Multicast routing for mobile ad-hoc networks using swarm intelligence" International Journal of Recent Trends in Engineering, Vol 1, No. 1, May 2009.

[3] Benamar Kadri, Djilalli Moussaoui, and Mohammed Feham "A pki over ant colony based routing algorithms for manets –antpki" International Journal of Network Security, Vol.15, No.1, PP.42-49, Jan. 2013

[4] Nada M. A. Al Salami, "Ant Colony Optimization Algorithm", UbiCC Journal, Vol. 4, No. 3, pp. 823-826, 2009

[5] Bibhash Roy, Suman Banik, Parthi Dey, Sugata Sanyal and Nabendu Chaki, "Ant Colony based Routing for Mobile Ad-Hoc Networks towards Improved Quality of Services", Journal of Emerging Trends in Computing and Information Sciences, Vol. 3, No. 1, pp. 10-14, 2012.

[6] Gunes M, Kahmer M, Bouazizi I. "Ant Routing Algorithm (ARA) for Mobile Multi-Hop Ad-Hoc Networks - New Features and Results", The Second Mediterranean Workshop on Ad-Hoc Networks. 2003

[7] Marwaha S, Chen Kong Tham, Dipti Srinivasan "Mobile agent based routing protocol for Mobile Ad hoc Networks". IEEE Global Telecommunications Conference (GLOBECOM ' 02) Taipei, Taiwan , 2002.

[8] Hossein O, Saadawi T. "Ant Routing Algorithm for Mobile Ad Hoc Networks (ARAMA)" 22nd IEEE International Performance, Computing and Communications, Conference, Phoenix, Arizona USA, pp. 281-290,2003.

[9] B. Kadri, A. Mhamed, and M. Feham, "A new management scheme of cluster based PKI for ad hoc networks using multi-signature", IEEE Global Information Infrastructure Symposium, pp.167-172,2007.

[10] B. Kadri, M. Feham, and A. Mhamed, "Securing reactive routing protocols in MANETs using PKI (PKIDSR)",The Journal of Security and Communication Networks, vol. 2, no. 4, pp. 341-350, 2008.

BIOGRAPHY

T.Pertreesia Maria is pursuing M.E (Applied electronics) in Sathyabama University, Chennai. She completed her B.E in Electronics and Communication in 2008 from Loyola institute of Technology, Chennai. Her field of interest includes mobile adhoc network and wireless communication.

A.Aranganathan M.Tech., (Ph.D) is working as a Assistant professor in the department of Electronics and Telecommunication Engineering in Sathyabama University, Chennai for the past six years. His field of interest is mobile agents, multicast routing in adhoc networks, network security.