A Two Way ACO approach to Identify Next Secure Promising path in MANET

Dinesh Kumar
Student, Mtech (CSE), Deptt. Of CSE
Lovely Professional University,
Phagwara, Punjab, India

Supreet Kaur
Asstt. Professor, Department of CSE
Lovely Professional University,
Phagwara, Punjab, India

Abstract— **A Mobile network is one of the most busy network on which lot of different kind of data in different formats travels. As the number of the users increases over the network, performing a secure transmission over the network is a great challenge. A Mobile network always sufferes from the problems of bad nodes as well as the high congestion over the network. In such case some mechanism is required to perform the communication from a secure path. The presented work is about to identify a compromising path so that the reliable communication can be performed. The presented work is divided in two main stages first to detect the nodes that perform heavy data loss because of some attack or the congestion. Once the nodes detected a safe path will be identified by using Ant Colony Optimization. The proposed work will reduce the network loss and improve the communication over the network.**

Keywords- ACO, Bad Node, Congestion, Compromising Path, MANET

I. INTRODUCTION

A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless [1]. It is a set of wireless devices called wireless nodes, which dynamically connect and transfer information. Each node in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently; each must forward traffic unrelated to its own use, and therefore be a router. The MANET network enables servers and clients to communicate in a non-fixed topology area and it’s used in a variety of applications and fast growing networks [2]. With the increasing number of mobile devices, providing the computing power and connectivity to run applications like multiplayer games or collaborative work tools, MANETs are getting more and more important as they meet the requirements of today’s users to connect and interact spontaneously.

MANET is vulnerable to different kind of attacks due to no clear secure boundary. The nature of MANET, nodes have the freedom to join and leave inside the network. Node can join a network automatically if the network is in the radio range of the node, thus it can communicate with other nodes in the network. Due to no secure boundaries, MANET is more susceptible to attacks. The attacks may be passive or active, leakage of information, false message reply, denial of service or changing the data integrity. The links are compromised and are open to various link attacks. Attacks on the link interfere between the nodes and then invading the link, destroying the link after performing malicious behavior. There is no protection against attacks like firewalls or access control, which result the vulnerability of MANET to attacks. Spoofing of node’s identity, data tempering, confidential information leakage and impersonating node are the results of such attacks when security is compromised[3].

Some of the attacks are to get access inside the network in order to get control over the node in the network using unfair means to carry out their malicious activities. Mobile nodes in MANET are free to move, join or leave the network in other words the mobile nodes are autonomous [4]. Due to this autonomous factor for mobile nodes it is very difficult for the nodes to prevent malicious activity it is communicating with. Ad-hoc network mobility makes it easier for a compromised node to change its position so frequently making it more difficult and troublesome to track the malicious activity. It can be seen that these threats from compromised nodes inside the network is more dangerous than attacking threats from outside the network.

A. SECURITY IN MANET

Security in Wireless Network is the most important concern for the basic functionality of network. Availability of network services, confidentiality and integrity of the data can be achieved by assuring that security issues have been met. MANET often suffer from security attacks because of its features like open medium, changing its topology dynamically, lack of central monitoring and management, cooperative algorithms and no clear defense mechanism. These factors have changed the battle field situation for the MANET against the security threats. In the last few years, security of computer networks has been of serious concern which has widely been discussed and formulized. Most of the discussions involved only static and networking based on wired systems. However, mobile Ad-Hoc networking is still in need of further discussions and development in terms of security [5]. With the emergence of ongoing and new approaches for networking, new problems and issues arises for the basics of routing. With the comparison of wired network Ad-Hoc network is different. The routing protocols designed majorly for internet is different from the mobile Ad-Hoc networks (MANET). Traditional routing table was basically made for the hosts which are connected wired to a non dynamic backbone [6]. Due to which it is not possible to support Ad-Hoc networks mainly due to the movement and dynamic topology of networks. Due to various factors including lack of infrastructure, absence of already established trust relationship in between the different nodes and dynamic topology, the routing protocols are vulnerable to various attacks [7]. Major vulnerabilities which have been so far researched are mostly these types which include selfishness, dynamic nature, and severe resource restriction and also open network medium. Despite of the above said protocols in MANET, there are attacks which can be categorized in Passive, Active, Internal, External and network-layer attacks, Routing attacks and Packet forwarding attacks. MANET work without a centralized administration where node communicates with each other on the base of mutual trust. This characteristic makes MANET more vulnerable to be exploited by an attacker from inside the network. Wireless links also makes the MANET more susceptible to attacks which make it easier for the attacker to go inside the network and get access to the ongoing communication [8, 5]. Mobile nodes present within the range of wireless link can overhear and even participate in the network.

II. EXISTING WORK

In this section we will give a short overview of existing work and entry points to the literature. Many different types of attacks have been proposed so far. [9], proposes a security solution for manets using a pre-existing routing protocol, ad hoc on-demand vector routing (aodv), using password security for each routing node and timeliness to update routing table. In [10], the approach involves the use of finite state machines for specifying correct AODV routing behaviour and distributed network monitors for detecting run-time violation of the specifications. In [11], focus is on achieving the routing and secure data exchange in a single step. A work on worm hole prevention is performed in[12]. . The scheme relies on the idea that usually the wormhole nodes participate in the routing in a repeated way as they attract most of the traffic. Therefore, each node will be assigned a cost depending in its participation in routing. Besides preventing the network from the wormhole attack, the scheme provides a load balance among nodes to avoid exhausting nodes that are always cooperative in routing. In [13] a method of worm holed detection and avoidance is defined. In proposed solution, if sender wants to send the data to destination, firstly it creates a secure path between sender and receiver with the help of verification of digital signature. If there is presence of any malicious node in between the path then it is identified because malicious node does not have its own legal digital signature.

In year 2006, Yih-Chun Hu has defined a work on worm hole attack in sensor network. According to his work In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively)to another location, and retransmits them there into the network.[14] This paper present a general mechanism, called packet leashes, for detecting and, thus defending against wormhole attacks, and we present a specific protocol, called TIK, that implements leashes. To defend against the wormhole attack, [15] propose a timing-based countermeasure that avoids the deficiencies of existing timing-based solutions. Using the proposed countermeasure, the nodes do not need synchronized clocks, nor are they required to predict the sending time or to be capable of fast switching between the receive and send modes. Moreover, the nodes do not need one-to-one communication with all their neighbours and do not require to compute a signature while having to timestamp the message with its transmission time.

A theoretical analyses of simple wormhole routing algorithms, showing them to be nearly optimal for butterfly and mesh connected networks. Our analysis requires initial random delays in injecting messages to the network[16]. Since the wormhole network **is** a popular communication system used in the new generation of large-scale parallel multiprocessors, real-time communication support on wormhole networks becomes an important issue. In this paper to evaluate a priority mapping scheme, a priority adjustment scheme and a message dropping method **for** large-scale real-time wormhole networks. The priority mapping scheme embeds the timing property of a message into a priority **for** flow control decisions. The priority adjustment scheme dynamically modifies the priority of a message as the timing property of the message changes[17].

A Cryptography based approach is applied to secure a network from wormhole attack. The proper wormhole detection will then be applied to suspicious links by means of an exchange of encrypted probing packets between the two supposed neighbours (endpoints of the wormhole). Our solution has several advantages since it does not require any time synchronization or location information and shows high detection rate under various scenarios[18].

III. PROPOSED ALGORITHM

When we find the alternate path, we have to fulfill the following constraints:

(a) Maximum path length (MaxLen)

MaxLen represents the maximum acceptable length of a path defined as the sum of edge weights wi in the path. The path length may represent various physical properties, such as distance, cost, delay, or failure probability. It can be represented by i, an integer or a float value. If wi = 1 is true for all edges, then the path length is the hop number from a source to a destination.

(b) Maximum number of hops on the path (MaxHop)
MaxHop represents the maximum acceptable number of hops on a path. If a path contains k nodes, then its hop number is k-1. MaxHop is an integer value.

(c) Maximum number of shared edges (MaxSE)
Shared edges among three paths, also called common edges, include two types of edge sharing: double-shared and triple-shared edges, respectively. We use integer values MaxSEdbl and MaxSEtri to denote the related maximum acceptable number of double-shared and triple-shared edges. This constraint is essential in cases requiring high network reliability when multiple paths are used between two routers.

The proposed alternate path scheme can now be formulated as:

```
1.  Establish a network with N number of nodes
2.  Specify the properties of network in terms of
    transmission, topology specification, forwarding ratio,
    load etc.
3.  Define the Source and the Destination Node over the
    network
4.  Define the m Bad Nodes over the network
5.  Each Node Ni start Moving in Direction of Specific
    Direction Di
6.  Find M Neighbor Nodes of Nodes Ni and Maintains the
    respective Information
    For (j=1 to M)
    {
    MaintainFormation (Ni,Nj)
    }
7.  if DataLoss(Ni)>Threshold and TimeDelay > Threshold1
    /* If Bad Node or Congested Node Occur on Node i*/
    {
    For i=1 to Mi
    {
    CollectInformation(Ni, Neighbor(Ni));
    }
    }
8.  implement Forward ANT to find the alternate path in each
    Direction of Neighbour(N(i)).
9.  Set the Pheramon on Each Hop and Identify the Possible
    Path
10. Implement Backward ANT to inform Neighbour odes
    about Backup Path
11. Trace the Pharamons and Commmunicate of ew Path
12. Perform the Normal Communication
}
```

The algorithm does not assumes a predefined network topology i.e. network is initialized first and then the maximum amount of data to be sent over the network or we can simply say data packet size as well as maximum elapsed time for defining network lifetime has to be stated. All the constraints defined in the above section have to be taken into account before applying the proposed algorithmic scheme.

In this present work we have improve the path selection algorithm by using the concept of Ant colony optimization. The first step is to setup the network with specific parameters. These parameters includes

a. Number of Packets : This property represents the number of successful packet delivery for a specific communication.
b. Number of Packet loss : Due to the congestion or any block node there are the chances of the data loss over the network. This parameter will analyze the packet loss over the transmission. It is the decision parameter that will perform the analysis the next node is a valid node or not.
c. Packet Delivery Ratio : This parameter is basically defines the ratio of packets transmitted and the packet successfully arrived to the destination. The packet delivery ratio we have analyzed on 4 intermediate nodes to identify the problem area over the network.

IV. CONCLUSION

The shortest path is used to transmit sensory data over the mobile networks. The existing algorithm for finding this shortest path was given by Dijkstra which is not intruder safe and easily fall prey to intruder attack.
As the shortest path is more prone to intruder attack, an alternate path which is secure from intruder attack would be developed because intruder would be interested in shortest path, it won’t be having any information about its existence. The proposed work is identify a secure path using ACO approach. We have defined a Two way ACO to generate a secure and efficient path for data transmission over the network.

REFERENCES

[1] http://en.wikipedia.org/wiki/
[2] P. Padmanabhan, 1. Gruenwald, A. Vallur, and M. Atiquzzaman, "A Survey of Data Replication Techniques for Mobile Ad hoc Network Databases," *The VLDB Journal - The International Journal on Very Large Data Bases*, vol. 17, pp. 1143 - 1164,2008.
[3] D.B.Roy, R.Chaki and N.Chaki, “A New Cluster-Based Wormhole Intrusion Detection Algorithm for Mobile Ad-Hoc Neworks,” International Journal of Network Security and Its Application (IJNSA), Vol. 1, No.1, April, 2009.
[4] N.Shanti, Lganesan and K.Ramar, “Study of Different Attacks on Multicast Mobile Ad-Hoc Network”.
[5] K. Biswas and Md. Liaqat Ali, “Security threats in Mobile Ad-Hoc Network”, Master Thesis, Blekinge Institute of Technology” Sweden, 22nd March 2007
[6] G. A. Pegueno and J. R. Rivera, “Extension to MAC 802.11 for performance Improvement in MANET”, Karlstads University, Sweden, December 2006
[7] S. Lu, L. Li, K.Y. Lam, L. Jia, “SAODV: A MANET Routing Protocol that can Withstand Black Hole Attack.,” International Conference on Computational Intelligence and Security, 2009.

[8] P.V.Jani, “Security within Ad-Hoc Networks,” Position Paper, PAMPAS Workshop, Sept. 16/17 2002

[9] Suman Deswal and Sukhbir Singh, “Implementation of Routing SecurityAspects in AODV”, InternationalJournal of Computer Theory and Engineering, Vol. 2, No. 1 February,2010.

[10] Chin-Yang Tseng, “A Specification-based Intrusion Detection System for AODV”.

[11] Monis Akhlaq, “Addressing Security Concerns of Data Exchange in AODV Protocol”, World Academy of Science, Engineering and Technology 16 2006.

[12] Mariannne. A. Azer, “Wormhole Attacks Mitigation”, 2011 Sixth International Conference on Availability, Reliability and Security

[13] Pallavi Sharma Prof. Aditya Trivedi, “An Approach to Defend Against Wormhole Attack in Ad Hoc Network Using Digital Signature”, 978-1-61284-486-2 IEEE.

[14] Yih-Chun Hu, “Wormhole Attacks in Wireless Networks”, I EEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006

[15] Majid Khabbazian,” Severity Analysis and Countermeasure for the Wormhole Attack in Wireless Ad Hoc Networks”, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS 1536-1276/09@ 2009 IEEE.

[16] Sergio Felperin,” A Theory of Wormhole Routing in Parallel Computers”, 0-8186-2900-2/92@1992 IEEE

[17] Jong-Pyng Li,” Priority Based Real-Time Communication for Large Scale Wormhole Networks”, 0-8186-5602-6/904 1994 IEEE

[18] Farid Na¨ıt-Abdesselam,” Detecting and Avoiding Wormhole Attacks in Optimized Link State Routing Protocol”, WCNC 20071525-3511/07©2007 IEEE