Improved Friend Communication Using Classifier Technique in MANETS-IFCCT

[1]S. Kumuthadevi, [2]Neethu Mariam Joseph
[1]M.E Student, Karpagam University, Coimbatore
[2]M.Tech Assistant Professor, CSE, Karpagam University, Coimbatore

Abstract-Improved friend communication using classifier technique in Manets(IFCCT) is an algorithm to provide secure routing in ad-hoc mobile networks. We propose this scheme that has been drawn from a network of friends in real life. The algorithm works by sending challenges with proper evidence report and based on that rating the friend nodes and sharing friend lists to provide a list of trusted nodes to the source node through which data transmission finally takes place. The nodes in the friend list are rated on the basis of the amount of data transmission they accomplish and their friendship with other nodes in the network.As a result of this scheme of operation the network is able to effectively isolate the malicious node by using classifier technique which describes the evidence report generation to avoid cheating which are left with no role to play in the ad-hoc network. One major benefit of this scheme is that the nodes do not need to promiscuously listen into the traffic passing through their neighbors. The information about the malicious nodes is gathered effectively by using challenges and evidence reports. This reduces the overhead on the network significantly. The results are simulated on IFCCT and it provides an efficient approach towards security and easier detection of attacker nodes in MANETS.

I. INTRODUCTION

WIRELESS technologies have revolutionized the world of communications. It started with the use of radio receivers or transceivers for use in wireless telegraphy early on; and now the term *wireless* is used to describe technologies such as the cellular networks and wireless broadband Internet. The wireless medium has limited spectrum along with a few other constraints as compared to the guided media, it provides the only means of *mobile communication*. Wireless ad hoc networking is used for random and rapid deployment of a large number of nodes, which is a technology with a wide range of applications such as tactical communications, disaster relief operations, health care and temporary networking in areas that are not densely populated. A mobile ad-hoc network (MANET) [1]–[3] consists of mobile hosts equipped with wireless communication devices. The transmission of a mobile host is received by all hosts within its transmission range due to the broadcast nature of wireless communication and Omni-directional antennae. If two wireless hosts are not within the transmission range in ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks among the mobile hosts in the deployed area. The use of wireless ad hoc networks also introduces additional security challenges that have to be dealt with. The weak links that cause these security challenges are as follows.

A. Easier to Tap

Since the media is nothing but air, it can be tapped easily.

B. Limited Capacity

The wireless medium has limited capacity and therefore requires more efficient schemes with less overhead.

C. Dynamic Nature

The self-forming, self-organization and self-healing algorithms required for ad hoc networking may be targeted to design sophisticated security attacks.

D. Susceptibility to Attacks

The wireless medium is more susceptible to jamming and other denial-of-service attacks.

Attacks in MANETs can be broadly classified as: passive and active attacks. In passive attacks the intruder remains undetected and captures the data while the message is being transmitted over the network. Eavesdropping and traffic analysis mainly fall in this category. Unlike passive attacks, in active attacks the intruder/attacker can affect the communication by modifying the data, misleading the nodes in the network. As a matter of fact, various scenarios and threats can be developed based on these approaches.

In this paper, we present the design and propose an algorithm to establish secure routing in mobile ad-hoc networks by implementing classifier. We use trust establishment through friends and challenges for authenticating nodes with proper evidences and reports .This provides a mechanism for isolating malicious nodes in the network .So this system checks the trustiness of the user continuously. It takes less bandwidth on the reporting, the algorithm tackles all the security challenges in an innovative way and gives a robust mechanism without the need of any central authority.

II. RELATED WORK

This section discusses the previous work done in the field of secure routing in ad hoc networks. The goals of any secure routing protocol are to provide some or all of the properties such as Authentication, Access control, Confidentiality, Privacy, Integrity, Authorization, Anonymity, No repudiation, Freshness, Availability, Resilience to attacks. Of these, Availability in particular targets denial of service (DoS) [5] attacks and has the ability to sustain the networking functionalities without any interruption due to security threats. The routing algorithms deal with the dynamic aspects of Mobile Ad Hoc Networks in their own way depending upon the requirements of the system. Essentially a routing algorithm can behave in a reactive, proactive, or a combination of both, that is, in a hybrid way. Reactive algorithms are those that behave in an on-demand fashion, which means that these algorithms gather routing information in response to some event viz. start of a data session, route request messages, link failure messages etc. Proactive algorithms are those which gather essential information before hand, so that the information is readily available when an event occurs. Hybrid algorithms use both proactive and reactive components in order to try to combine the best of both schemes. The conventional routing protocols for MANETS are DSR [4] and AODV [6].A number of routing protocols have been proposed towards providing security in ad hoc networks. Some of the most widely discussed protocols are Authenticated Routing for Ad Hoc Networking (ARAN) , ARIADNE and Watchdog Path rater. There have also been various secure routing techniques that use multipath based routing where they break the data into different number of sub packets, encrypt them and then finally route them through different paths.

In this work we have looked into the secure routing techniques and have designed the proposed IFCCT protocol to provide better security. These protocols have been discussed in the following subsections, as these protocols are the ones that have been used for comparison with the proposed technique IFCCT.

III. IFCCT PROTOCOL

In this section we discuss our proposed algorithm in detail. The proposed system is an enhanced FACES for neighbor estimation for secure routing in MANET. As discussed in the previous chapter the major limitations of FACES are trusted relationship. The project is to provide a solution for trust relationship in user rating in MANET environment. IFCCT algorithm is divided into four stages, viz. *Challenge Your Neighbor, Rate Friends, Share Friends and Route through Friends* as described in fig1.

The proposed system employs FACES Algorithm stages of implementation on routing a data from source to destination. The whole system is divided into five modules. The first module deals with topology creation and challenge your neighbor, the second module checks and rate the neighbors. The third module for sharing friends details fourth module do the routing through the friends. The fifth module handles the implements the classifier to check for evidences in friend's rating. The proposed system is implemented in NS2 with MANET extension.

A. Block Diagram

The overall dataflow diagram for the proposed system is given in Fig1

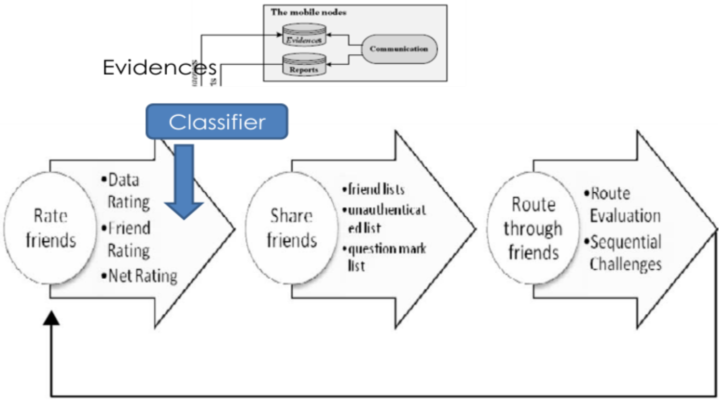

Fig.1: Proposed Idea

B. List of Modules

Module1: Topology Creation and Challenge the Neighbor

1. A MANET is created with a suitable topology. The Challenge response system is implemented to check for the user authenticity by following steps:
2. When the network is newly initialized, each node is a stranger to another. Thus each node incorporates its neighbors in the *unauthenticated list*.
3. The node A picks one of the neighbors, B and performs the usual *Share Friends Stage.*
4. As a response the neighbor node B either sends its friend list or the nodes from its *unauthenticated list* if the friend list is empty.
5. On receiving the list, the node A picks up a node which it can reach on its own and in the most efficient way. Let us say that this node is C.
6. Now the node has two ways to reach the node one through and another through a route already known to it.

7. The node initiates a challenge and encrypts it with the public key of C. It then sends it through both routes. A also includes its own public key with the challenge.
8. The node B sees the challenge as a normal data packet and routes it. As C decrypts the data packet and finds that it is a challenge it responds to the challenge. It then encrypts the response with 's public key that it obtained in *STEP 6*.
9. A receives the result of the challenge from both routes and after decrypting, it compares them. If they are same then node A adds node B at the bottom of its friend list.

Module 2: Rate Friends

Friends are rated on at the successful completion of the challenge acceptance of node. Initially each node has only those nodes in their friend list that completed the challenge successfully. Friend relation is transitive in nature that is if is A a friend of B and B is a friend of C, A includes in his friend list C too. Each friend in the list has the following three classes of ratings: *Data Rating (DR)*, *Friend Rating (FR)* and *Net Rating (NR)*.

Data rating: The data rating is updated by a node for its friend on the basis of amount of data it transfers for it. This is a significant metric for judging the quality of the node.

Friend rating: During the *Friend Sharing* stage, since the friends are transitive the rating also shares among the friends. E.g A a node asks for the friend list of node C and incorporates the rating of friends also.

Net rating: FR represents the opinion of the friends of a particular node towards the integrity of another node, while DR represents a personal opinion of a node derived on the basis of previous data sessions. Both these ratings are important as certain nodes could be selectively malicious. By combining these two values we arrive at a more holistic metric called as the Net Rating

Module 3: Share Friends

Friend sharing is a periodic process which is chiefly responsible for the security of the algorithm. To accomplish friend sharing we use the control packet *FREQ* (Friend sharing request). The node receiving the *FREQ* replies with the nodes in its friend list, unauthenticated list and the question mark list.

Module 4: Routing through friends

Data routing through friends takes places as follows.

1. When a node wants to transmit to a particular destination, it initiates a Route Request message within the network. It includes the number of data packets to be sent in the Route Request option
2. When it receives the Route Reply messages from the network. It evaluates the route available to the destination node on the basis of its friend list. The Route Reply messages contain the public key of the destination node. The public key and private key pair is randomly generated at the source and destination nodes.
3. It routes data through the best possible route and waits for a back-off interval to obtain an acknowledgement of the number of data packets received by the destination. Destination uses multiple routes to transfer this information to the source node, so that it is received positively.
4. If the source finds that the number of data packets received at the destination is equal to the amount that it sent, it increases the Data Rating of the nodes in the path, for which it is a friend as discussed in the Friend Rating section.
5. If the source finds that some data packets were dropped or receives no acknowledgement from the destination it initiates a *Sequential Challenge*.
6. If the results of the *Sequential Challenge* indicate that a particular node was deliberately misbehaving, it terminates that node from its friend list and moves it to the question mark list.
7. If all nodes complete the challenge successfully, the source infers that there is some data loss due to unintended behavior. This happens as a packet from the destination is initiated which indicates the number of data packets received. This packet follows the original path to source and each node attaches the number of packets it had transferred to its neighbor node.
8. On receiving the packet, the source can evaluate that packet loss had occurred at which nodes, and it decreases the rating of the nodes in its friend list as discussed in section pertaining to Data Rating

Module 5: Implement Classifier to check for Evidences

Classifier is implemented to receive the reports from the mobile nodes. Evidence is defined as information that is used to establish proof about the occurrence of an event or action, the time of occurrence, the parties involved in the event, and the outcome of the event. The purpose of an Evidence is to resolve a dispute about the result from data transmission. The Evidence contains two main parts called DATA and PROOF. The DATA part describes the user credentials, i.e., node address, time, data, and contains the necessary data to regenerate the nodes' signatures. The PROOF is an undeniable security token that can prove the correctness of the DATA and protect against payment manipulation, forgery, and repudiation.

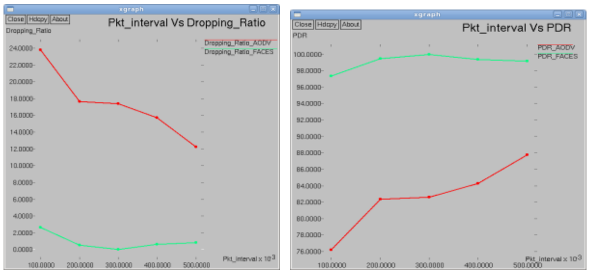

Fig.2: Number of data packets dropped by malicious nodes versus mobility and Packet intervals with PDR.

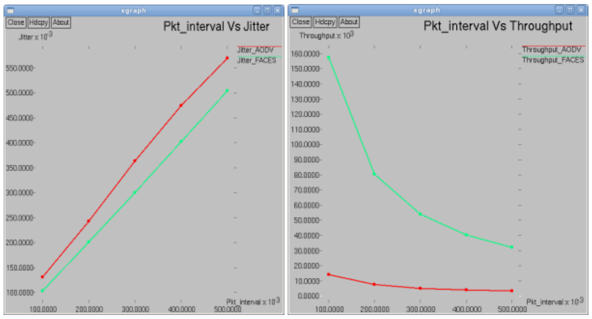

Fig.3: Packets interval Vs Jitter and packet interval Vs throughput

IV. RESULTS AND DISCUSSION

The execution environment was Network Simulator version 2, Fedora on an Intel Core2Duo processor, 4 GB RAM machine. The simulation result for the proposed algorithm is shown in figures. It shows that existing nodes and a new nodes wishes to join the network. First new node tires to connect with existing node, then that node get the assistance of next node. It sends key to previous node and a new node. Then previous node checks the key from new node for authentication. Then based on the evidence report of new node it should be accepted as friend node or else it will be rejected as malicious node. Figure shows that the routing takes place from source to destination which has high rating value.

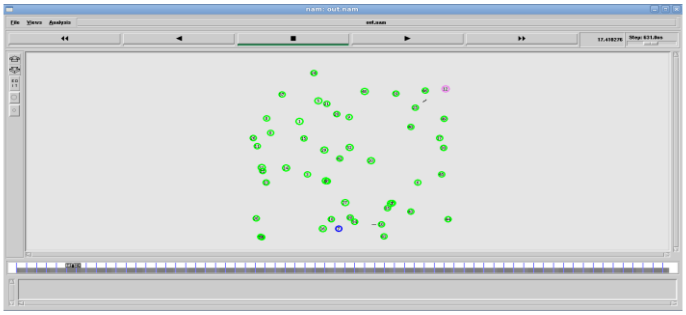

Fig.4: Neighbor challenging

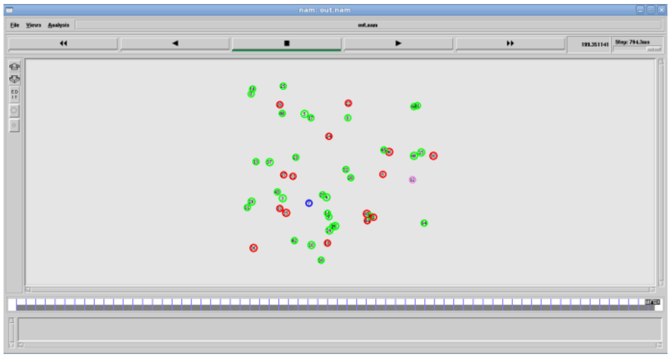

Fig.5: Malicious node detection

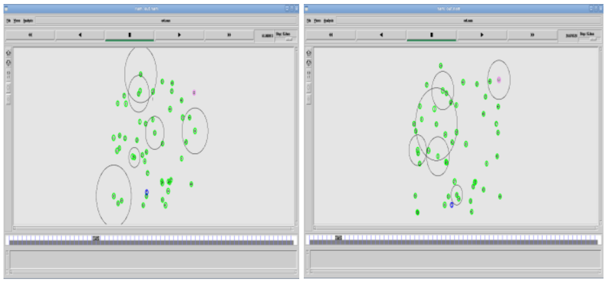

Fig.6: Routing through Nodes

The proposed IFCCT protocol uses challenge authentication which helps in detecting all the attacks mentioned .This is explained as follows: *Dropping Data Packets, Dropping Control Packets, Modifying IP Datagram, Flooding, Wormhole, Gray hole, Spoofing, Grudge War.*

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed IFCCT, a robust scheme for node authentication by making as a friend with proper evidence report in the MANET systems. And also this is used to avoid malicious nodes by identification of cheating nodes. Our analytical and simulation results explain the IFCCT can significantly reduce the communication and processing overhead comparing to existing schemes. Moreover the proposed algorithm can provide security and identify the cheating nodes precisely and rapidly. And it is used to minimize the probability of dropping the messages, improve the network performance in terms of throughput and packet delivery ratio. In the future, we plan to implement existing secure routing protocols and compare them with the proposed IFCCT protocol. This would give a better picture about the standing of the proposed algorithm.

VI. REFERENCES

[1] Aikaterini Mitrokotsa, Christos Dimitrakakis(2012), Intrusion detection in MANET using classification algorithms: The effects of cost and model selection, ScienceDirect, Adhoc Networks, 2012

[2] Deepak Verma, Renu Jain, Ashwani Kush (2013), A comprehensive study of latest security models for MANETs:

Covering Intrusion Detection and Denial of Service Attacks, International Journal of Computing and Business Research (IJCBR) ISSN (Online): 2229-6166, Volume 4 Issue 1 January 2013

[3] Geethu Bastian, Arun Soman(2013) EFS: Enhanced FACES Protocol for Secure routing in MANETs, International Journal of computer science Engineering and Technology, 2013

[4] Mohamed M. E. A. Mahmoud and Xuemin (Sherman) Shen, Fellow, IEEE(2013), A Secure Payment Scheme with Low Communication and Processing Overhead for Multihop Wireless Networks, Parallel and Distributed Systems, IEEE Transactions on Volume:24 , Issue: 2, 2013

[5] Sanjay K. Dhurandher, Mohammad S. Obaidat, Fellow, IEEE, Karan Verma, Pushkar Gupta, and Pravina Dhurandher (2011), FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems, IEEE SYSTEMS JOURNAL, VOL. 5, NO. 2, JUNE 2011

[6] S.V.Shirbhate Dr. S.S.Sherekar Dr. V.M.Thakare (2013), Technical Analysis of Intrusion Detection in Routing Protocol for Mobile Ad Hoc Network, International Journal Of Computer Science And Applications Vol. 6, No.2, Apr 2013

[7] S. Shantha Meena, V.S. Shankar Sriram(2013), Route Challenging Scheme Using Friend Based Rating in MANETs, International Journal of Engineering and Technology, Vol 5 No 2 Apr-May 2013

[8] The Network Simulator NS2, http://www.isi.edu/nsnam/ns/ns-build.html,2010.