Journal of Computer Science Engineering and Software Testing
Volume 4 Issue 1

Establishing Security in Manets Using Friend-Based Ad Hoc Routing Algorithms

Aparna. C[1], Dr Nelson Kennedy Babu[2] , Radha. S[3]
[1]Assistant Professor, Sengunthar College of Engineering
[2]Professor/CSE, Dhanalakshmi College of Engineering, Coimbatore
[3]Assistant Professor, Sengunthar Engineering College
E-Mail: aparnait@gmail.com[1], cnk_babu63@gmail.com[2],radhai1984@gmail.com[3]

Abstract

Establishing security in MANET is challenging issue in any adhoc routing protocol. Neighbor nodes do not updated their routing status and bandwidth consumption during the transmission. AODV used single chain topology so bandwidth offers single chain transmission. To establishing the secure transmission FACES provide new challenges to its neighbor. Proposed system incorporate cache update and aware of routing information this scheme that has been drawn from a network of friends in real life scenarios. This algorithm send request in the form of challenges and sharing nearby neighbor lists to provide trust worthy nodes to the source node through which data transmission finally takes place. Proposed system taking various packet sizes into their account and deals only best effort traffic and AODV used only simple priority algorithm. Due this algorithm network can easily identifies the malicious node and provide secure neighbor node detection in the mobile adhoc network.

Index Terms: *Secure based friend list Ad Hoc Routing, Network connectivity, Neighbor coverage, simulation analysis.*

INTRODUCTION

WIRELESS nodes consist of a collection of mobile nodes which can move freely. There is no fixed infrastructure and node can be dynamically self-organized into arbitrary topology networks. Many routing protocols, such as Adhoc on-demand Distance Vector Routing (AODV) has been proposed for MANETs. It does not require central point to handle the routing process and loop free that share higher bandwidth to its neighbor. They can also reduce control message overhead by keeping the address into the packet. AODV can reduces the node energy and also increases the delay. Thus finding the neighbor node through some challenges to reducing the overhead in route discovery and improve the energy level in network. MANET has colluding nodes it causes internal attack in adhoc routing and security. Suppose if two different nodes are not in its transmission range then other node can located between these nodes and send the reply to other neighbors. Due to this issue node can check their transmission range to all other neighbor nodes. Wireless networks introduce security challenges and deal with weak links that causes the following security issues.

1. ***Easier to Tap:*** Since the media is nothing but air, it can be tapped easily.
2. ***Limited Capacity:*** The wireless network has limited capacity therefore it requires efficient schemes with less overhead.
3. ***Dynamic Nature:*** The self-forming, self-organizing nature. Therefore special design may be need for security attacks.
4. ***Susceptibility to Attacks:*** Attacks in MANETs are passive and active.

Objective

Proposed system mainly designed for

establishing the security in mobile adhoc networks. Friend based adhoc routing mainly use trust establishment through friends and send some special challenges for authenticating nodes. Node can send the request to the neighbor node along with the challenges, friends updating the routing information and identify the authenticate nodes using this challenges. FACES tackle all the security challenges and give self-sustaining security without need of any central control.

Overview

The proposed FACES protocol accomplishes establishment of friends same as real life scenarios. When people meet in a new community or group they are strangers to one another. For trusting one another initially send challenges to the neighbor node, number of successful task completions with the trust level increases. Several trust relations are formed as a group and transfer the information to one another. The FACES algorithm is divided into four stages, viz. Challenge Your Neighbor node, Rate Friends list, Share neighbor and Route through Friends. The first and second stages are periodic, while third and fourth are on demand. Node initially sends challenges to the nearby neighbor node, which node have completed their challenges they are placed in the friend list. The nodes that do not complete the challenges they are shifted into query list, or the list of nodes are consider as a malicious nodes.

RELATED WORK

Proposed Adhoc on demand distance vector protocol (AODV) is specifically for use in multi hop wireless adhoc networks of mobile nodes. The protocol adapts quick routing changes when frequent node movement, yet requires small or less overhead when nodes move less frequent. The protocol used two mechanisms are route discovery and route maintenance, which working together and allow nodes to their transmission. AODV is a reactive protocol, the routes are initiated only on demand .It uses traditional routing table, one entry per destination and sequence number to determine whether routing is up to date and to prevent unwanted loop routing. The goals of secure routing protocol are provide authentication, access control, confidentiality, privacy, and integrity. Denial of service (DoS) [5] attacks has proposed the ability to sustain the network functionalities without any interruption due to security threats .In an routing algorithm network consists of number of nodes which communicate each other over a wireless channel. Some of the wireless networks have a wired backbone with only the last hop being wireless. Adhoc routing deal with the dynamic aspects and own way depending upon the requirements. Essentially a routing can behave like a reactive, proactive or combination of both. AODV behave in a reactive fashion. Reactive algorithms gather the routing information in response i.e. RREQ, link failure and data session. The conventional methods of routing protocols are DSR [4] and AODV [6].These conventional routing algorithms do not provide security and are prone to attacks caused by malicious nodes moving in the network. Due to this issue security is one of the major problems in adhoc network. Several security schemes are used in adhoc routing they are security based, payment based, reputation based and cryptography based systems. All methods are having their own functionality. Cryptography based method are one of the most widely used systems like public key, RSA and Diffie– Hellman [7], [8]. A number of routing protocols [9] have been proposed towards providing security in ad hoc networks. Some of the security protocols like Authenticated Routing for Ad Hoc Networking (ARAN) [9], ARIADNE [10]. The proposed system introduces FACES protocol to provide better security using these techniques.

PROPOSED PROTOCOL

Proposed approach combines the advantages of neighbor coverage knowledge and good neighbor detection which can significantly decreases the number of transmission. So as to reduce routing overhead and also reduces the energy consumption. In this section FACES introduces some of the list to check whether the neighbors are trustworthy. By using these information source node can start the routing process. To prevent the attacks list of terms are used in protocol as follows,

List of Terms Used

Question Mark List: The list of nodes which are do not completed the task within the duration.

Unauthenticated List: The list of nodes does not have a security.

Friend List: The list of Trust worthy nodes.

FREQ: Friend Sharing Request is used to initiate friend sharing. A node receiving this packet replies with the nodes in its friend list, unauthenticated list and the question mark list.

DR: Data Rating given to nodes after they transmit some amount of data for the source node.

FR: Friend rating is computed when nodes share their friend lists.

NR: Net Rating is computed as a weighted mean of DR and FR.

OR: Obtained Rating received during the friend sharing stage.

FACES Algorithm Description

Friend based Ad hoc routing using Challenges to Establish Security (FACES) accomplishes in the same way as in real life scenarios. Proposed systems used to develop the FACES algorithm are divided into the following four Stages as shown in Fig. 1(b): Challenge your neighbor, Rate Friends, Share Friends and Route through friends. The figure shows the link/flow between the different stages of the algorithm only on demand. But initially stages of challenges, friend sharing and rating are periodic processes. This makes the FACES protocol a hybrid one.

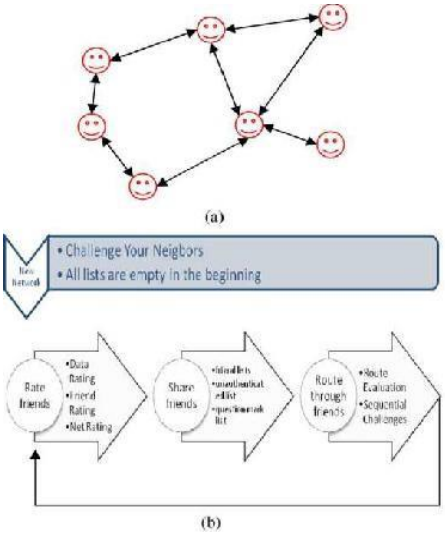

Fig.1. *(a) Network of friends in a community*
(b) FACES: Link/Flow between different stages.

Node initiates the route discovery process through Hello message to their neighbor nodes; all other neighbors are replying the same path. Based on the reply source node calculate the time duration, this calculation based on total transmission range is compare to number of node connected to the transmission path. If AODV (HELLO, RREQ, RREP) etc., received from node that has no entry in routing table then signal to noise ratio is measured, when the packet was received must be higher than a certain upper limit(threshold value) otherwise AODV is ignored. Neighbor in the routing table signal to noise ratio must be higher than a certain lower limit, otherwise AODV is ignored. This process is done only the initial stage of challenges finally node gather data about each other and populate a reliable friend list

Challenge your neighbor: Challenge is a mechanism to provide authentication to their neighbor. Figure shows how the challenge is initiated by A to B and it's disguised as a data packet for C. The

challenge is routed from D to C. Finally node calculates the arrival time from B to other node.

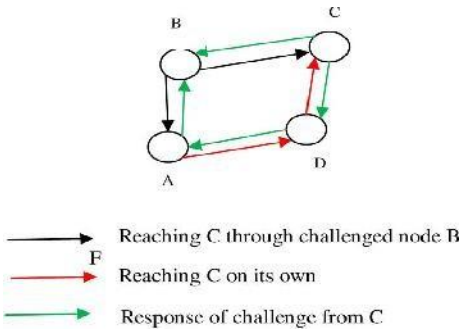

Fig.2. *Illustration of the challenge.*

Rate friends: Friend rates are normally from 0 to 10.During the route discovery processes each and every node should complete the task for further transmission. Sharing of friend nodes is done in the Share Friends stage as the friend relation is transitive in nature that is if A is a friend of B and B is a friend of G\ A includes C in his friend list 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 neighbor. Each node calculates the neighbor node information based on successful data transmission, and this metric is used to identify the node quality, capacity, signal strength. The data rating varies according to the number of data transferred the data packets. When a node drops data packet then source node compute the negative value rating of DR. Node can change the value of A according to the volume of data that is transferred trough the network. Keeping a value (of 1/100) ensures a smooth scaling from 1 to 10 for data packets up to 200 with a data rating of around 6 for 100 packets. As a value of A is increase, the curve increases DR quickly towards the maximum value 10. Value A is decreased then smoothens DR packet range.

Data Routing Through Friends

When source node wants to transmit a data packet to particular destination, then the node initiates a Route Request message within the network, it includes the number of data packets to be sent in the Route Request option. When a source node receives the Route Reply messages from the network then each node evaluates the route interval between data send and received. To provide additional security node uses public key and private key send along with the data packet. This process used to give more security for node selection process.

SIMULATION ANALYSIS:

The simulations analysis was carried out using the Qualnet simulation package Scenarios are

Node:—The number of Nodes in the simulation is changed for five scenarios for all protocols.

Mobility: The pause time of the node in simulation is varied for five scenarios for all protocols.

When there is a more number of nodes are isolated in the network then FACES uses these challenges to deduct the threats. Figure 3 and 4 shows greater number of malicious detection behaviors. Fig 5 shows that FACES perform better than other protocols. Lesser packets are routed the malicious nodes, it implies that FACES has better security characteristics. As we increase the number of nodes or mobility, we see more number of packets are transmitted through malicious nodes. Fig 6 presents the packet overhead with varying number of nodes and mobility in the network. This packet overhead parameter shows how heavy or how busy the networks and establishing the security. In the Figs 7 and 8, we can see that the packet drop is minimal in FACES, as it efficiently discards malicious nodes.

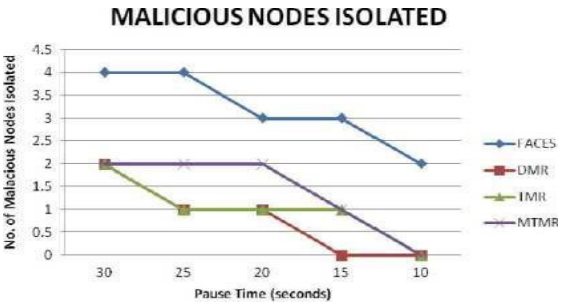

Fig. 3. *Number of malicious nodes detected versus mobility*

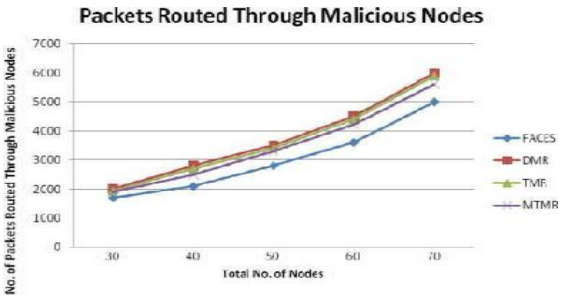

Fig. 4. *Number of packets routed through malicious nodes versus number of nodes.*

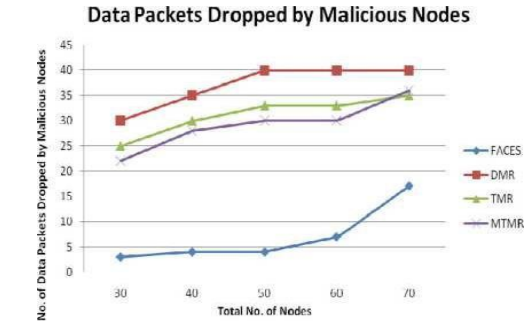

Fig. 5. *Number of packets routed through malicious nodes versus mobility.*

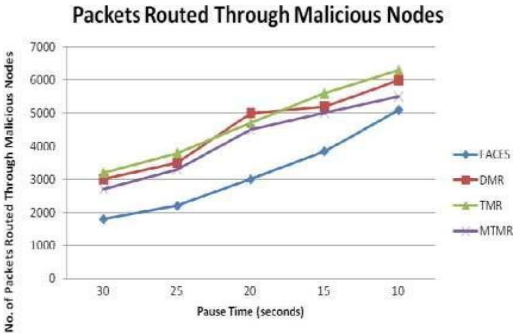

Fig. 6 *Number of control packets versus mobility*

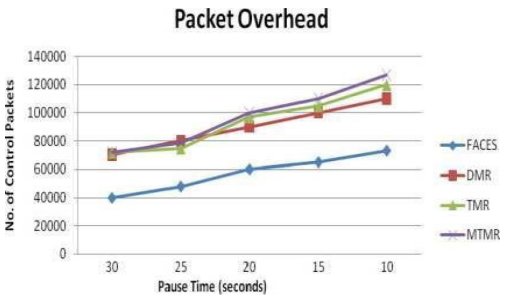

Fig. 7. *Number of data packets dropped by malicious nodes versus mobility.*

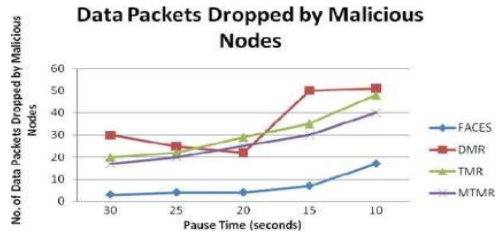

Fig. 8. *Number of data packets dropped by malicious*

CONCLUSION AND FUTURE WORK

The Proposed FACES algorithm is provides more security mechanism for mobile adhoc networks and give better performance. The simulation result compared to other routing protocol. The friends sharing scheme used to find a trusted node. Using a challenges node can easily identify the malicious node and provide authenticate any node compared to other security protocol. If adhoc network uses multipath routing algorithms then it will take more time to detect malicious node but FACES which detects activity by checking the challenge reply. There are many open questions in case of maintain the energy level such as quality of service guarantees, adaptability and security in future. A new optimization technique or energy efficient protocol may use to measure the signal quality and adaptability in mobile adhoc network. The proposed algorithm provides dynamic routing, less overhead and energy efficient routing protocol. Figure shows comparison table between FACES parameters with other routing protocol.

COMPARING FACES WITH DMR, TMR, AND TMTR

ATTACKS HANDLED	FACES	DMR	TMR	MTMR
Dropping Data Packets	Yes	Yes	Yes	Yes
Dropping Control Packets	Yes	Yes	Yes	Yes
Modifying IP Datagram	Yes	No	No	No
Flooding	Yes	No	No	No
Wormhole	Yes	No	No	No
Gray hole	Yes	No	No	No
Spoofing	Yes	No	No	No

REFERENCES

1. D. P. Agrawal and Q.-A. Zeng, Introduction to Wireless and Mobile Systems. Pacific Grove, CA: Brooks/Cole, Thomson, 2002.
2. I. Chlamtac, M. Conti, and J.-N. Liu, "Mobile ad-hoc networking: Imperatives and challenges," in Ad-Hoc Networks. New York: Elsevier, 2003, vol. 1, pp. 13–64, No. 1.
3. L.Wang and N.-T. Zhang, "Locally forwarding management in ad-hoc networks," in Proc. IEEE Int. Conf. Communications, Circuits and Systems and West Sino Expositions, Jun./Jul. 2002, pp. 160–164.
4. D. Johnson and D. Maltz, "Dynamic source routing in ad hoc wireless networks," in Book Chapter inMobile Computing, T. Imielinski andH. Korth, Eds. Dordrecht, The Netherlands: Kluwer, 1996, pp. 131–181.
5. A. Wood and J. A. Stankovic, "A taxonomy for denial-of-service attacks in wireless sensor networks," in Handbook of Sensor Networks:Compact Wireless and Wired Sensing Systems. Boca Raton, FL:CRC, 2005, pp. 32:1–32:20
6. C. Perkins, E. Royer, and S. Das, Ad Hoc on Demand Distance Vector (AODV) Routing Jul. 2003, Internet experimental RFC 3561.
7. W. Diffie and M. E. Hellman, "New directions in cryptography," IEEE Trans. Inform. Theory, vol. IT-22, no. 6, pp. 644–654, 1976.
8. M. S. Obaidat and N. Boudriga, Security of e-Systems and Computer Networks. Cambridge, U.K.: Cambridge Univ. Press, 2007.