ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

Emergence of Challenge Mechanism in the Light of Existing Secure Routing Schemes in MANET

Geethu Bastian[1], Arun Soman[2]

Department of Information Technology, Rajagiri School of Engineering and Technology,
Rajagiri valley, Cochin, India[1,2]

Abstract— Mobile Ad-hoc Network (MANET) is a collection of mobile nodes which can form a network at any time and at anywhere. All nodes act as routers and help in forwarding data between any two. Security is a major concern in ad-hoc network. Due to frequent node movement, routing algorithms in wired network is not suitable for MANET. Several separate routing algorithms have been designed in MANET for data transfer. But the problem is due to the misbehaving nature of mobile nodes. If a node is of misbehaving nature, it can actively attack the network and also it will not use its own constrained resources for the use of others, but it will preserve them for itself. There are different security based routing schemes to prevent selfishness in MANET and thereby to make routing in ad-hoc network secure. They are Credit based, reputation based, Multipath Routing schemes, Cryptography based and Trust based schemes etc. This paper explores the concept of secure routing in ad-hoc network by preventing malicious nodes from routing using a mechanism called Challenge in FACES Algorithm and also to make a study of the existing secure routing schemes available in MANET.

Keywords— MANET, routing schemes, ad-hoc, Challenge

I. INTRODUCTION

MANET represents a way of organizing mobile nodes to form a network without any pre existing infrastructure. Due to the movement of nodes in the network, it is having a dynamically changing topology. In this multi-hop ad-hoc network, for forwarding data between a source and destination the intermediate nodes act as routers for forwarding the data. Security in MANET is a challenging task due to the need for Authentication, Confidentiality, Integrity, Availability, Non Repudiation etc. Since the wireless channel is accessible to both actual users and attackers, they are more prone to attacks than wired structure. The main security problem is due to the change in behaviour of mobile node. If a node is malicious in behaviour it can attack the network actively, whereas if it is selfish in nature it will not use its constrained resources for relaying packets for others, but instead use those for their own purpose [2]. We want to avoid these nodes in order to make a highly secure network.

Conventional routing algorithms for MANET are DSR and AODV, but security is lost in some cases. Different types of attacks are possible even on DSR and AODV. Route Discovery and Route Maintenance are two basic mechanisms in DSR protocol. A node can alter the discovered path due to its malicious behaviour. Also a selfish node can participate in route discovery very actively, but may not work during packet forwarding resulting in dropping of packets [1]. Another attack is in the form of broadcasting too many Route Requests which is the DoS attack and can make the network congested with Route Replies. In AODV also we are having different attacks like DoS, Black-hole, Worm-hole and Gray-hole etc [3]. A number of routing protocols came forward for the purpose of providing security such as ARAN, ARIADNE. But security is still a major issue in ad-hoc network.

Since security is a major concern in ad-hoc networks, new security based routing methods are needed. Different schemes are available for establishing secure routing by avoiding nodes with un-intended behaviour. Among them are Credit based, Trust based, Cryptography based, Reputation based schemes and Multipath routing schemes [4]. Mostly used schemes are Cryptography and Reputation based schemes. But still security is an issue. This paper explores the concept of secure routing in MANET by preventing nodes with un-intended behaviour. For this, it uses a mechanism called Challenge in FACES Algorithm for node authentication. The nodes which have successfully completed the challenge process will be only used for routing. A highly secure routing protocol is desirable for the actual implementation of a MANET. A new routing protocol that will function efficiently by avoiding malicious nodes in the network is FACES.

FACES stands for Friend based Ad-hoc Routing using Challenges to Establish Security in MANET Systems. FACES Algorithm comes under the domain of network security. Network security involves the authorization of access to data in network which is controlled by network administrator. FACES Algorithm establishes trust through friends and uses challenge mechanism for authenticating nodes. Challenge is a basic test for all nodes in the network to prove their behaviour.

II. EXISTING ROUTING SCHEMES

Different schemes are available for enabling secure routing in MANET Systems. Many of the currently using protocols are making use of it. The available secure

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

routing schemes are Credit based, Reputation based, Trust based, Cryptography based, multipath routing schemes etc. But even though these schemes are available, security is a challenging issue in ad-hoc network due to the presence of malicious nodes. Each scheme is having its own features. Mostly used schemes are Reputation based and Cryptography based schemes. The proposed FACES Algorithm mainly uses Cryptography based and Trust based scheme. RSA public key algorithm is used in operations. This paper gives a study of the existing secure routing schemes and the current Challenge mechanism.

A. Credit Based Schemes

Security is the main issue while considering routing in ad-hoc network. Routing will go on smoothly only when the nodes perform their functions honestly. So in-order to make them functional, this scheme is providing incentives for the nodes. It means the nodes get paid for providing services to another node. If a particular node wants the help of another one for relaying packet, then it has to pay for that service. In [5], the authors used the concept of beans for this packet transfer. The two models proposed by them are Packet Purse Model and Packet Trade Model.

1) The Packet Purse Model (PPM)

In this scheme the originator is the one who is responsible for forwarding packet to others. Before sending the packet to the desired destination the originator loads with a number of beans that are required to reach the destination. Beans are loaded inside the packet. Then the intermediate nodes in between the originator and the destination take beans from the packet and pile up the stock of beans. But the problem is if the distance to the destination is very high, more number of beans is needed for forwarding the packet by the originator. Also there may be a possibility of discarding a packet due to the lack of beans inside the packet. Figure 1 gives an overall view of the Packet Purse Model. But there are disadvantages for this scheme. They are as follows.

Demerits:

The Originator can under estimate or over estimate the number of beans in the packet. If the originator underestimates the number of beans, then the packet will not reach at the destination. Also there is a chance of overestimate this number, then the packet will arrive, but the originator loses the number of beans invested in the packet.

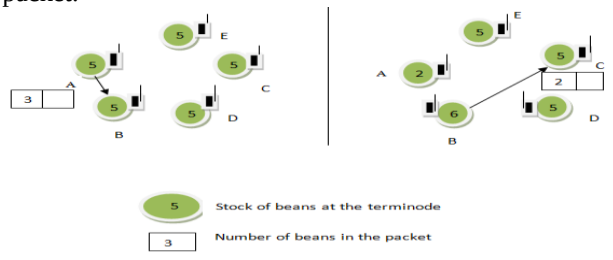

Fig. 1. Stages in Packet Purse Model

2) The Packet Trade Model (PTM)

In Packet Trade Model, destination pays for the packet forwarding service. In this method [6], each intermediate node that helps in packet forwarding increases the number of beans by buying and selling mechanisms. These nodes buy some beans from the previous nodes and sell it to next bean or destination for more beans. In the Packet Purse Model, beans are loaded inside the packet to be transferred. But here the packet does not carry beans. This is a main difference with the previous model. Figure 2 depicts the Packet Trade Model. Here the cost for packet forwarding is handled by the destination. In this example the intermediate nodes which help in forwarding increased their number of beans whereas the destination D decreased its number of beans.

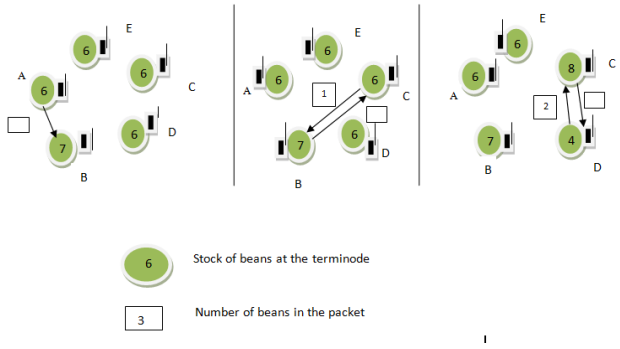

Fig. 2. The Packet Trade Model

This method is better than the Packet Purse Model. Here the originator does not want to bother about the number of beans that are required to reach the destination. Also this scheme is applicable in cases of multicast packets. A disadvantage is that this approach for charging does not directly deter users from flooding the network.

B. Reputation Based Schemes

In this scheme, the nodes in the network together detect the maliciousness of a particular node, and such detection is declared. This declaration is propagated throughout the network. So as a result, it will be removed from the rest of the network. In [7], the authors proposed 2 schemes. They are Watchdog and Pathrater. These are actually tools for detecting and mitigating routing mis-behaviour. Watchdog detects misbehaving nodes, whereas the Pathrater run by each node in the network combines two ideas and reach at a conclusion. It combines information of misbehaving nodes and reliability information about a link to pick the most reliable path. These two techniques can improve the throughput in ad-hoc network in presence of nodes that agree to do but fails.

1) Watchdog and Pathrater

The Watchdog technique is used to identify misbehaving n odes. It is implemented by keeping a storage space equivalent to a buffer of packets which have been sent recently. And these packets in the buffer are compared with the packets which are over-heard. This is made to check whether these are equal. If so, that particular packet is removed from the buffer, because it has been already forwarded. But if it is seen that it is there in the buffer for a longer time, then this scheme increases a counter for a node which is actually responsible for transmission. If this

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

counter exceeds a certain limit, then it is declared as malicious and this information is propagated. The main advantage of this method is it can detect misbehaving node. But in presence of false misbehaviour, limited transmission power this method fails.

Pathrater takes a highly reliable route by combining knowledge of selfish nodes and link reliability information. In this scheme each node in the network is having a rating for every other node present in network. Final selection of path is based on path- rating. If there exists a number of paths to the destination we choose the path with largest rating. Rating of path can be calculated by taking the average of rate of all nodes in that path. Pathrater assigns rating to a node according to the following scheme. A node rates itself with 1.0 always, if a particular node is known to the Pathrater it assigns the node with 0.5. Also it can increase or decrease the rating of a node.

If a node in a path is an active node, then Pathrater increase its rating by 0.01 at intervals of 200ms. We decrease a node's rating by 0.05 in case of any link break or unreachable condition. A path having a rating of negative value indicates the presence of selfish nodes.

C. Multipath Routing Based Schemes

The Secure routing techniques that are making use of multipath routing are DMR, TMR and MTMR [8]. DMR stands for Disjoint Multipath Routing. It takes the advantage of shortest path between the source and destination. TMR stands for Trust based Multipath Routing. TMR provides message security using Trust based Multipath Routing. MTMR which stands for Multipath and Message Trust based Routing. It uses a mechanism of assigning trust levels and update strategy to detect selfish nodes. Since this scheme relies on multiple paths, suppose a path is attacked by an intruder, it cannot be received by destination correctly. These 3 techniques are used in FACES Algorithm.

1) Security through Disjoint Multipath Routing (DMR)

For enhanced secure routing, initially a secure connection is established. After the establishment of secure connection between source and destination, this scheme will find out multiple routes between the source and destination using Dynamic Source Routing (DSR) [1]. Then the discovered routes sorted based on time taken for discovery of route. First the message to be transmitted is divided into parts. Then encrypt these 4 parts and send through four different routes. This scheme is highly secure, because for an attacker to get the original message all parts of the encrypted message are needed.

2) Trust based Multipath Routing (TMR)

This scheme defines trust levels, and upon these levels the nodes are get rated. The less trusted nodes are given less parts of the encrypted data content, so it makes difficult for an attacker to get the data. As the above scheme, this will also find out multiple routes using DSR Algorithm. Since each node is having a trust value, this scheme selects the route with maximum trust level. Trust levels are assigned in a range of -1 to 4. A trust level of 4 indicates a complete trust. If a node is having a trust level of 4, then it means the node is trusted and can route packets through these trusted nodes. Assignment of trust level to a node is dependent on its interaction with and suggestion from neighbours.

3) Multipath and Message Trust Based Secure Routing (MTMR)

As already said, this technique uses 2 techniques, Trust assignment and Trust Updating mechanisms. Here in this scheme, each node is given a trust level of 0. According to the behaviour of the node, trust levels are increased or decreased. Here the trust level ranges from -4 to 4. This scheme selects the path with highest trust level. Initially there may are multiple paths calculated using the algorithm DSR. After the path is selected data is transmitted through the selected path. Also this scheme uses a factor called T_Req, indicates the Trust Requirement of the message that decides how the content can be routed. Each and every data is having this parameter based on its content and type. Also it uses 2 parameters $A_m(t)$ and $A_p(t)$. $A_m(t)=2*|t|$, this indicates the allowed number of misbehaviours a node can perform. $A_p(t)=2^{|t|}$, gives the number of times a node can perform normal behaviour. Since this technique also rely on trust value, it makes the less trusted nodes difficult to get the message that is transmitted.

D. Trust Based Schemes

All nodes in the ad-hoc network is to be honest and cooperative to perform the network functions [9]. But this assumption is not always true. Malicious nodes are making use of this to attack the network actively in the form of DoS attack, man in the middle etc. Trust in MANET is divided into two [10]. They are Direct Trust and Recommender Trust. When there is no evidence for direct trust, recommender trust value is taken. In [11], uses a trust based scheme. The trust level assigned to a node is done by evaluating the recommendation from neighbour nodes and its direct interaction. The benefit of this scheme is that less trusted nodes will get less chance to authenticate. Based on the value of the trust nodes are selected for data transmission. If a node is [12] having a trust value lower than a predefined threshold, then it will not be considered for further route selection. It is important to note that information has to be masked from un-trusted nodes. Even though trust value is defined, we can't completely trust on this value given by peers.

FACES Algorithm is also making use of Trust based scheme, in a way that most trusted nodes are given to the source finally for data routing. These trusted nodes are finding out by the mechanism called Challenge and Share Friends stage.

E. Cryptography Based Schemes

Routing protocols mainly rely on Cryptography to establish security in ad-hoc network. Mainly used public key algorithms are RSA and Diffie-Hellman. In contrast to symmetric key cryptography, public key cryptography

ISSN (Print) : 2319-5940
ISSN (Online) : 2278-1021

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 2, Issue 6, June 2013

allows users to communicate securely without using a single secret key, but instead using a pair of keys called public and private key. The private key is the secret key and the public key is the global key. But even though they are mathematically related it is infeasible to find private key from public key. When RSA Algorithm is used attacks are possible [13]. They are Brute force attack, Timing attack and Mathematical attack etc. But even though it provides better confidentiality and also its a powerful Algorithm in Cryptography. In Diffie-Hellman Key Exchange scheme, there is a possibility of man in the middle attack.

III. THE CURRENT METHODOLOGY

FACES Algorithm comes under the domain of network security. FACES use Challenge mechanism to detect and isolate malicious nodes. This is an efficient mechanism for the nodes to prove their behaviour and thereby to authenticate themselves.

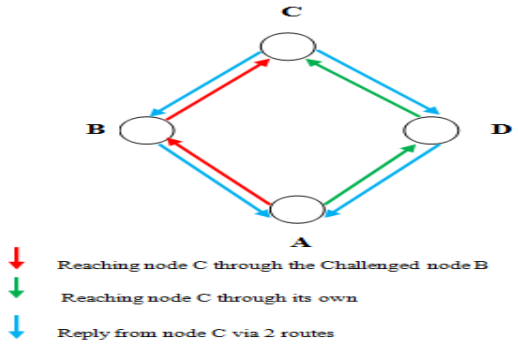

Fig. 3. Illustration of Challenge

When a network starts up, all nodes are strangers to each others, and then the algorithm puts all nodes in un-authenticated list. First all nodes start to share friend list. Since the friend list is empty initially, nodes share their unauthenticated list. The figure 3 depicts the Illustration of Challenge. Node A picks one of the neighbours from B's list in such a way that A could reach that particular node directly or through other node. Here the node A is challenging its neighbour B to check its behaviour. If a node does not respond to challenge, it is moved to question mark list, a list where suspicious nodes are kept. Node initiates a Challenge and encrypts it with public key of C, also A includes its own public key and sends it through both routes. C decrypts data it received performs computation on it, encrypt it with public key of A and sends the result through 2 paths. The Algorithm assumes that the response that the node A obtained through the route which it finds its own is always correct. Then A compares 2 results. If results are same, then node B is added to the friend list of node A. Otherwise B is added to the temporary list.

Description of Challenge

Each node is initialized with a pair of large prime numbers that are secret to that node. So A is done with (a, b) and C with (c, d). When A challenges node B, A sends a random prime number say 'n' to C through 2 routes. Node C computes c^d mod n and sends the result through 2 routes. A compares two results to reach at a conclusion on challenged node B. Here it is difficult to find c and d from mod function because n, c, d are large prime numbers. This is a highly efficient mechanism. It is very difficult for a misbehaving node to authenticate. To Share Friends in FACES Algorithm, initially challenge is needed to prove its correct behaviour.

IV. CONCLUSION AND FUTURE WORK

FACES offer a secure scheme to provide security in ad-hoc network. The Challenge mechanism is an efficient mechanism to detect and prevent malicious nodes. Friend Sharing scheme is also an effective method to spread information about trusted friends in the network because selfish nodes cannot differentiate a packet intended for challenge and real data. FACES scheme confirms a malicious node by checking the challenge reply. This scheme reduces overhead and routing through malicious nodes. When compared to the schemes available, even if each scheme is having its own features, security is a major issue in ad-hoc network. As a future work, it is possible to conduct challenge mechanism again on nodes in temporary list to make trusted in future. So that they can be used for data routing and can make them friends also.

REFERENCES

[1] Shayan Ghazizadeh, Okhtay Ilghami, Stefan Schlott, Evren Sirin, "Security-Aware Adaptive Dynamic Source Routing Protocol" , IEEE Conference on 6-8 Nov 2002
[2] Frank Kargl, Alfred Geiß, Stefan Schlott, Michael Weber, "Secure Dynamic Source Routing" , 38th Annual Hawaii International Conference on System SciencesPages:1-10
[3] Suman Deswal and Sukhbir Singh, "Implementation of Routing Security Aspects in AODV" International Journal of Computer Theory and Engineering, Vol. 2, No. 1 February, 2010
[4] Sanjay K. Dhurandher, Mohammad S. Obaidat, *Fellow, IEEE, Karan Verma, Pushkar Gupta, and* Pravina Dhurandher,' FACES: Friend-Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems' , IEEE SYSTEMS JOURNAL, VOL. 5, NO. 2, JUNE 2011
[5] L. Buttyan and J.-P. Hubaux. "Enforcing service availability in mobile ad-hoc wans", In *Proceedings of IEEE/ACM* Workshop on Mobile Ad Hoc Networking and Computing *(MobiHOC)*, Boston, MA, 2000..
[6] Mrs. K.Vijaya, "*Secure 2ack routing protocol in mobile ad hoc networks*", IEEE Conference, pages 1-7,2009.
[7] Sergio Marti, T. J Giuli, Kevin Lal and Mary Baker "Mitigating Routing Misbehavior in Mobile Ad-hoc networks", ACM/IEEE Conference,pages 257-259.
[8] Mohana, Dr.N.K. Srinath," Performance Analysis Of Secure And Trust Based Routing Algorithms For Mobile Ad-Hoc Network.". International Journal of Engineering Research and Applications, Vol. 2, Issue4, July-August 2012, pp.1213-1219
[9] K.Seshadri Ramana, DR. A.A. Chari, Prof. N.Kasiviswanath" A Trust-Based Secured Routing Protocol for Mobile Ad hoc Networks," Global Journal of Computer Science and Technology
[10]Alfarez Abdul-Rahman & Stephen Hailes" A Distributed Trust Model",
[11]Z. Liu, A. W. Joy, and R. A. Thompson, "A dynamic trust model for mobile ad-hoc networks"
[12]Edna Elizabeth. N., Radha. S., Priyadarshini. S., Jayasree. S. & Naga Swathi. K., " SRT-Secure Routing using Trust Levels in MANETs," European Journal of Scientific Research ISSN 1450-216X Vol.75 No.3 (2012), pp. 409-422
[13]William Stallings, "Cryptography and Network Security," Chapter 10.