EFS: Enhanced FACES Protocol for Secure Routing In MANET

Geethu Bastian
Department of Information Technology
Rajagiri School of Engineering & Technology, Rajagiri Valley P O
Kochi-39, India
geethubastian@gmail.com

Arun Soman
Department of Information Technology
Rajagiri School of Engineering & Technology, Rajagiri Valley P O
Kochi-39, India
arunnnediyasala@gmail.com

Abstract— Mobile Ad-hoc Network (MANET) is an autonomous system of mobile hosts equipped with wireless communication devices. These mobile nodes can form a network anywhere and at anytime. But the topology of the network thereby formed will be unpredictable due to frequent node movement. For sending data to destination, source node can send directly or can forward via an intermediate node depending upon the range of destination node. Since security is a major concern in ad-hoc network, secure routing algorithm is essential for MANET. Even if there are different algorithms to prevent selfishness in MANET and thereby to make routing in ad-hoc network secure, they have their own disadvantages. This paper explores the concept of a new algorithm which is an enhanced version of the existing FACES Algorithm that routes data on the basis of trust. The Trust is evaluated by conducting a Challenge scheme. This is an efficient scheme that can isolate malicious nodes and also it can make them trust worthy. This algorithm is also having several other significances. This paper will also make a study of the existing routing scheme FACES.

Keywords-MANET; malicious; Challenge

I. INTRODUCTION

An ad-hoc network is a collection of two or more devices equipped with wireless communication devices. It is a network without any pre-existing infrastructure. So it is easy to deploy. Due to the frequent movement of nodes, ad-hoc network is having an unpredictable topology. For the transfer of data between a source and destination, there are several routing schemes. But they all are having their own disadvantages. Since the wireless channel is accessible to both original users and the attackers, they are more prone to attacks than the wired architecture. If a node is malicious in behavior 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[1]. So there should be a simple, reliable and efficient protocol for the secure transfer of data. FACES protocol is an algorithm which can be used for the same purpose. It is an algorithm that comes under the domain of network security. In order to prevent unauthorized access, modification or denial of computer network, certain policies are adapted by the network administrator. Network security consists of these policies and all.

The conventional algorithms that are used for routing are Dynamic Source Routing (DSR) and AODV. But these will not provide absolute security, attacks can happen. In DSR when a source node wants to transmit data to a destination node, the entire route to destination will be included in the packet header. So the nodes in between the source and destination can use this route to understand whether to whom the packet is to be transferred. But in this Algorithm, there is a possibility of invisible node attack. It means malicious node can participate in route request and route reply forwarding. But their real intention is different. Also a malicious node can alter the route in the packet header; it can drop packets during routing even if it behaves normally while in the discovery phase. DoS attack is also possible in DSR [2]. AODV, which is an on-demand routing protocol is also having the two phases called Route Discovery and Route Maintenance. In AODV also we are having different attacks like Black-hole, Worm-hole, and Gray-hole etc [3]. In Black hole attack, an attacker can project it as having a shortest path to destination; thereby source node sends the packets through this attacker node. Whereas in Gray hole attack, an attacker node may forward all Route Requests and Route Reply packets. But they will not forward all the data packets. In AODV, Dos attack results when the network bandwidth is hijacked by malicious node [3].

In the existing FACES Protocol, routing of data is on the basis of trust. It routes data only to the node having largest number of trusted friend nodes. This Algorithm uses a mechanism called Challenge to detect and isolate

malicious nodes. But the algorithm does not provide a scheme for improving these malicious nodes. It is a major fault of this existing algorithm. Once they are detected as malicious, they will be completely avoided from the routing process. In the enhanced version of FACES Algorithm there is giving an opportunity for the malicious nodes to get improve. It is a major advantage of this new version. Also the new version offers many other features that the existing one doesn't have. The new algorithm uses shortest path algorithm to forward Challenge and data packets. This also improves the efficiency of the new algorithm. Also for the authentication of nodes in the network instead of prime number assignment, a new mechanism has derived in the new version which will further improve the security of the system. Thus the new routing protocol will function efficiently by making the malicious nodes in the network good and trust worthy. So they can be used for the further data forwarding.

II. EXISTING ROUTING SYSTEM

The existing Algorithm is FACES which stands for Friend based Ad-hoc routing using Challenges to Establish Security in MANET. The Algorithm is used to establish network of friends, this establishment can be compared with the real life. The Algorithm comes under the domain of network security. In order to prevent unauthorized access, modification or denial of a computer network and network accessible resources, certain policies are adapted by the network administrator. Network security consists of these provisions and polices. The Algorithm is having 4 phases. They are Challenge the neighbour, Rating of Friends, Share Friends and route through Friends. The Algorithm uses the way of trust establishment through friends and for node authentication it relies on a mechanism called Challenge.

The Algorithm establishes a network of friends in ad-hoc network that helps for the final routing. This establishment can be compared with that we seen in the real life. Initially when people meet in a society, they will be completely strangers. Since no one has any information about others with malicious intention, we can trust them completely in the initial stage. We will trust one another based on the completion of tasks successfully. These trust relationships leads to the formation of community [4].

Initially the nodes are subjected to the Challenge mechanism. Figure 1 gives an illustration of Challenge scheme. The information about the malicious nodes can be effectively obtained during this stage. This stage helps us to efficiently isolate those nodes.

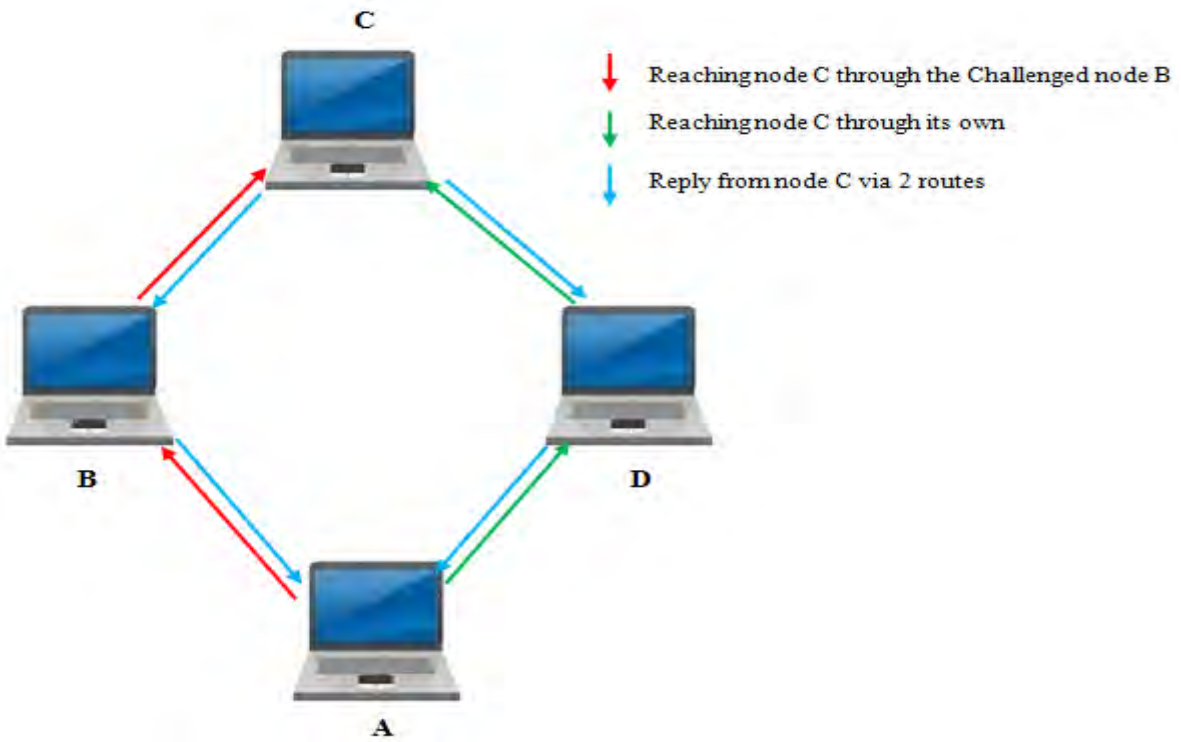

Figure 1: Illustration of Challenge

Initially node creation is done. The nodes in the network are then initialized with a pair of prime numbers. In the algorithm it uses large prime numbers to initialize for each node. The assigned numbers are secret to each node. These numbers are further used in sending challenge packet. Challenge is a basic test that the nodes have to be cleared before they enter into the routing procedure. But the algorithm is giving a chance only for the detection of misbehaving nodes. Once the nodes are found as malicious, then they will be moved to a list called

temporary list. Then they are not given a chance to improve. So it can't get into the friend list of source node again. This is a major fault of this algorithm. In the enhanced version of the FACES Algorithm, the nodes in temporary list are given a chance again so that they can improve and thereby can take part in routing.

Challenge is a test for the nodes to prove its honesty. We want to check whether a particular node is misbehaving or not at a certain time period. So what we want to do is to select a source and destination. Source node is responsible for sending one of its random prime number in encrypted form to the destination node. Public key cryptography is used for encryption and decryption. Destination receives the encrypted data, decrypts it and performs a computation on it. Computation includes a mod operation. The mod operation outputs the remainder. So the destination is supposed to send back the result to the source node. This can be called as the Direct Challenge scheme.

Now we are going to Challenge the intermediate node. Now an intermediate node comes in between a source and destination. Here now the source sends the random prime number in encrypted form to the intermediate node. And this intermediate node is responsible for sending the same to destination. The Intermediate receives the challenge data, decrypts and send it to the destination. It sends it to destination in encrypted form. The receiver node then again receives it, decrypts and performs computation. If the intermediate is a malicious node, it can perform some malfunction in the received data before sending to the receiver node. Then receiver sends back the result to the source node. Source checks the two results. The Algorithm works on the assumption that the result of direct challenge will be always true. So if the 2 results are not equal, the intermediate node is moved to the temporary list. But the algorithm is not giving a chance for this intermediate node to be trust worthy. Also here the intermediate node is selected in a random fashion. We can name any node as intermediate. It does not use any algorithms for finding the nearest node to transfer this challenge packet [5].

In the Rating phase, a node is rated based on its behaviour during Challenge procedure, also based on the account of friendship to other nodes. It is called Data rating and friend rating respectively. Algorithm also calculates net rating which is the weighted mean of data and friend rating. The rating of a node gives an idea of how good a node is.

In the Share friend's stage, which is the next phase of the Algorithm, a source is supposed to share its friend list with the destination. The friend list of source will contain only those nodes which have completed the Challenge successfully. So we can assure that friend list will only contain friends of the source node. So it is secure to share that list with destination. Also thereby destination can get more trusted friends. The first three stages which are the Challenge, rating, sharing are all periodic events in the Algorithm. But the next phase which is the Routing of data is on demand. In the routing stage, source node routed data to the most trusted destination. The trust is evaluated on the basis of number of friends it has. Destination node will be the only node having larger number of friends. Only after completing the first 3 stages which are periodic events the routing will be done. So the Source sends data to the destination [4].

III. RELATED WORK

In [6] Marti et al. describes two techniques that improve throughput in ad-hoc network in presence of nodes that agree to forward packets, but fail to do so. The two techniques are Watchdog and Path rater. Watchdog identifies misbehaving nodes by maintain a buffer of recently sent packets and comparing each over-heard packet with that in buffer to verify if there is a match. If a packet has remained in buffer for a longer time watchdog increments failure tally for the node which is responsible for forwarding, and if this tally exceeds a threshold bandwidth it determines that the node is misbehaving. Path rater combines the knowledge of misbehaving nodes and link reliability data to pick the reliable route.

All nodes in the ad-hoc network is to be honest and cooperative to perform the network functions. 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. In [7] Zheng Yan et al. a Trust Evaluation based security solution is proposed. It uses a Trust evaluation Matrix considering experience statistics, personal preference, references etc. This is resistant to DoS and Black hole attacks. In [5], provides a routing mechanism using challenge scheme. Isolation of selfish nodes can be done using this. But it is also vulnerable to attack. In [8], a dynamic trust model is introduced. Initially every node is assigned a trust value. Then it dynamically updated the trust value based on the reports from threat detection tools like Intrusion detection system located on all nodes. When a node is found as malicious by its neighbor, it will initiate a trust report and propagate it. Source node uses the trust level for route evaluation. In [9], it proposes Secure Routing using Trust levels in Node Transition Probability (NTP) protocol. It calculates T_{rate} for each node and classifies them into three lists. They are Ally list, Associate list and Acquaintance list. The nodes in Ally list are those responsible for sending highly secure information. The nodes which are grouped under Associate list are those which are meant for sending information with moderate security. The nodes in Acquaintance list are those used to send data which do not need any security. 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.

IV. THE PROPOSED SYSTEM

The Proposed system is an extension of the existing algorithm FACES. FACES stands for Friend based Ad-hoc routing using Challenges to Establish Security in MANET. FACES protocol which comes under network security offers security through a mechanism called Challenge. The enhanced version is a simple, reliable and efficient protocol for implementing security in ad-hoc network. Several new changes are implemented for the newer version to make it efficient in every sense.

The Algorithm is having the same 5 phases. They are Node Creation, Challenge the neighbour, Rating a node, Sharing Friend list and finally Routing of data. After the creation of nodes in network, each node has to be assigned with a pair of prime numbers which will be secret to each node. Initially when the network is newly initialized, the predecessor and successor of each node is assigned as its friend nodes. Only after the Challenge scheme, a node will come to know who all its real friends are. The assignment of these prime numbers is needed because of the computation need to be performed in Destination. Now it's time to find the neighbours of the source node, So that it needs to challenge only those nodes and can prove its behaviour. In the existing scheme source is allowed to challenge any node in a random fashion without considering any distance and bandwidth parameter. But it's not a good practice to do the same to any node. So the new Algorithm has provisions to find a shortest path to the destination node. So that it needs to Challenge only those nodes in between them.

The distance of a vertex say 'd' from a vertex 's' is the length of the shortest path between 's' and 'd'. Shortest path means minimum length from one node to another. For this the Dijkstra's Algorithm computes the distances of all the vertices from a start vertex's'. The Dijkstra's algorithm is based on Greedy method. It adds vertices in the order of increasing distance. So we have to assume that the graph is connected, the edges are undirected and the edge weights are non negative. Dijkstra's algorithm is better if only a path from a single node to another or to all others is needed. After the successful implementation of Dijkstra's algorithm, Challenge is to be performed. But this time, we want to challenge only those nodes in the shortest path. To a particular destination, there may exists only a single shortest path from the source.

After the selection of source and destination perform the direct Challenge as described in the existing system. Source node is responsible for storing the result of the direct Challenge. Then have to select the nearest intermediate node. It has to be selected according to the obtained shortest path. Then perform the Challenge via the intermediate node. It will reveal the behaviour of the intermediate node. As in the existing scenario, the malicious nodes can be easily caught using this method. So that it can be moved to the temporary list. But the existing FACES Algorithm is not giving any opportunity for the nodes in the temporary list to improve. But the newer version is giving a second chance for these nodes. So that it can improve their behaviour.

Giving a second chance means allowing the malicious nodes to prove their identity. So we can conduct a Challenge operation again via the malicious node that lies in temporary list. So at this time it is found that the node behaves normally. So it is moved to the friend list of source node. Again continue the Challenge operation with the next intermediate node in the shortest path. If it is a malicious node, do the same as above. Otherwise it is moved directly to the friend list. It is possible to implement TESLA (Timed Efficient Stream Loss-tolerant Authentication) protocol for sending Challenge packet to all intermediate nodes simultaneously and can save time to check each intermediate separately. It can also be used for the authentication of source. The TESLA Algorithm is implemented as a separate unit apart from EFS. TESLA is based on loose time synchronization between sender and receiver. For this sender can generate a one way key chain. The key chain is generated by randomly selecting s_l and repeatedly applying the function F. The sender reveals the values in the opposite order. One key per time interval is used. After the determination of time interval, sender uses a function of the corresponding key at that interval as a cryptographic key for the computation of MAC. The key for source authentication is generated by applying another function on the corresponding key in keychain at that interval. For sending the first packet in a newly created network, the sender first generates MAC over the contents of the packet. The content to be transferred is the secret data of the sender. Sender sends Data, MAC and Key to the receiver. The receiver verifies MAC and ensures Message Integrity. Through the verification of key, source can be authenticated. The key used for source authentication and MAC Generation are different. This is an efficient algorithm for authentication. Due to the presence of MAC codes we can also ensure about the safety of data. So TESLA offers better security [10].

In the next phase, which is the Rating we can obtain the rating of a node under 3 categories. According to the behaviour of node during the Challenge, data rating can be obtained. According to the friendship of the node with others, Friend rating can be calculated. And finally net Rating can be calculated as the weighted mean of data and friend is rating. Evaluation of a node based on this rating is done by source and destination. The net rating of an intermediate node given by destination is important, because that particular node will be used to forward data to destination.

In the Share Friends stage source node is allowed to share its friend list with the destination. To prove that the source node is engaged in sharing, in the new algorithm source sends its secret prime number to the destination in encrypted form.

In the Routing phase of the Algorithm, source node tries to route data to the trusted destination. The trust level of destination is evaluated on the basis of number of friends a destination has. Through sharing of friend list with the destination, destination will be the only one node having larger number of friends. So it is possible to trust the destination node. So source routes data to the most trusted destination through the most trusted intermediate node according to the net rating of that intermediate node.

The newer version of the Algorithm is offering many features that the existing one doesn't have. The use of Dijkstra's algorithm is one among them. By this, source node needs to challenge only those who are lying closest to source node. By giving the malicious nodes a chance to improve, source node is expanding its friend list which leads to the expansion of friend list of destination through the Sharing phase of the algorithm. By the implementation of TESLA, source node can send the data securely to the destination due to the presence of MAC code and key.

V. CONCLUSION AND FUTURE WORK

Enhanced FACES Algorithm offer a secure scheme to provide security in ad-hoc network. The Challenge mechanism is an efficient mechanism to detect, prevent and to improve the malicious nodes. Friend Sharing scheme is also an effective method to spread information about trusted friends in the network. The new algorithm also confirms a malicious node by checking the challenge reply. This scheme reduces overhead and routing through malicious nodes. Only after making the false nodes a good one, they are added to the friend list. When compared to the existing schemes available, even if each scheme is having its own features, since security is a major issue in ad-hoc network, the newer version is offering the best security. As a future work, TESLA protocol can be implemented within the Challenge stage. That is TESLA protocol which is a broadcasting protocol can be used to broadcast the challenge packet among the intermediate nodes. So it will enhance the security of the whole system. It is possible to implement reactive algorithms like DSR and AODV to collect routing information in response to events like start of a data session. Also can use large random numbers for node assignment, for the computational purpose logarithmic function can be used to simplify mathematical calculation.

REFERENCES

[1] Frank Kargl, Alfred Geiß, Stefan Schlott, Michael Weber, "Secure Dynamic Source Routing" , 38th Annual Hawaii International Conference on System SciencesPages:1-10

[2] Shayan Ghazizadeh, Okhtay Ilghami, Stefan Schlott, Evren Sirin, "Security-Aware Adaptive Dynamic Source Routing Protocol" , IEEE Conference on 6-8 Nov 2002

[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] Shobana M', Companion Based Mechanism To Establish Secure Routing In MANETs Systems', International Conference on Computing and Control Engineering (ICCCE 2012)

[6] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. MobiCom '00, 2000.

[7] Zheng Yan, Peng Zhang, Teemupekka Virtanen, "Trust Evaluation based Security Solution in Ad Hoc Networks".

[8] Zhaoyu Liu, A. W. Roy, R. A. Thompson,' A dynamic trust model for mobile ad hoc networks' , 10th IEEE International Workshop on Future Trends of Distributed Computing Systems.

[9] 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 .

[10] Adrian Perrig, Ran Canetti, J. D Tygar, Dawn Song, 'The TESLA Broadcast Authentication Protocol'.