Volume 3, Issue 7, July 2013 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Efficient Secured Multicasting Routing Protocol in MANET

Renu Chaudhary
GIMT, KURUKSHETRA
India

Sahil Batra
ASSTT. PROFESSOR, GIMT,KUK
India

Amit Chaudhary
INTRALINKS INC. BOSTON, MA
India

Abstract— MANET is one of the most common ad hoc network with lot of problems related to congestion and routing. We are providing one of the solutions to secure the transmission over the network. Security aspects play an important role in almost all of the application scenarios given the vulnerabilities inherent in wireless ad hoc networking from the very fact that radio communication takes place (e.g. in tactical applications) to routing, man-in-the-middle and elaborate data injection attacks. Security has become a primary concern in order to provide protected communication between mobile nodes in a hostile environment. This paper proposes secured multicast routing protocol in MANET. Firstly we have to find out the shortest path between source nodes and various destination nodes and then imply the security in multicast routing. This prevents wastage of time and cost. The keys are exchanged with the help of GDH(Group Diffie-Hellman Algorithm with n-parties) and the Encryption and Decryption of data is done with the help of RSA Algorithm. This proposed scheme will improve the performance of the network such as delay and packet delivery ratio than traditional routing algorithm.

Keywords— MANET, multicasting, DBF , GDH, RSA

I. INTRODUCTION

A MANET is a system of wireless mobile nodes that dynamically self-organize in arbitrary and temporary network topologies[1]. People and vehicles can thus be internetworked in areas without a preexisting communication infrastructure or when the use of such infrastructure requires wireless extension. In the MANET, nodes can directly communicate with all the other nodes within their radio ranges; whereas nodes that not in the direct communication range use intermediate node(s) to communicate with each other. In these two situations, all the nodes that have participated in the communication automatically form a wireless network, therefore this kind of wireless network can be viewed as MANET.Wireless applications, like emergency searches, rescues, and military battlefields where sharing of information is mandatory, require rapid deployable and quick reconfigurable routing protocols, because of these reasons there are needs for multicast routing protocols[2]. There are many characteristics and challenges that should be taking into consideration when developing a multicast routing protocols, like: the dynamic of the network topology, the constraints energy, limitation of network scalability, and the different characteristics between wireless links and wired links such as limited bandwidth and poor security. Generally there are two types of multicast routing protocols in wireless networks. Tree-based multicast routing protocol. In the tree-based multicasting, structure can be highly unstable in multicast ad-hoc routing protocols, as it needs frequent re-configuration in dynamic networks, an example for these type is MAODV and ADMR. The second type is mesh-based multicast protocol. Mesh-based multicast routing protocols are more than one path may exist between a source receiver pair, CAMP and ODMRP are an example for these type of classification.

II. DISTRIBUTED BELLMAN-FORD

Distributed Bellman Ford[3] also known as Distance Vector Routing Algorithmis a well known shortest path routing algorithm with time complexity of O(|V||E|) where,V – vertices,E – edges.The DBF algorithm was developed originally to support routing in the ARPANET. A version of it is known as (Routing Internet Protocol) RIP[3] and is still being used today to support routing in some Internet domains. It is a table-driven routing protoco1, that is, each router constantly maintains an up-to-date routing table with information on how to reach all possible destinations in the network. For each entry the next router to reach the destination and a metric to the destination are recorded. The metric can be hop distance, total delay, or cost of sending the message. Each node in the network begins by informing its neighbours about its distance to all other nodes. The receiving nodes extract this information and modify their routing table if any route measure has changed. For instance, a different route may have been chosen as the best route or the metric to the destination may have been altered. The node uses the following formula to calculate the best route:

$$D(i, j) = \min [d(i, k) + D(k, j)]$$

where D(i,j) is the metric on the “shortest” path from node i to node j , d(i, k) is the cost of traversing directly from node i to node k, and k is one of the neighbours of node i. After recomputing the metrics, nodes pass their own distance information to their neighbour nodes again. After a while, all nodes/routers in the network have a consistent routing table to all other nodes.

III. GROUP DIFFIE-HELLMAN ALGORITHM

GDH[4][5] is a contributory key agreement protocol which is essentially an extension of the two party Diffie-Hellman protocol. The basic idea is that the shared key is never transmitted over the network. Instead, a list of partial keys (that can be used by individual members to compute the group secret) is sent. One member of the group-group controller-is changed with the task of building and distributing this list. The controller is not fixed and has no special security privileges. The initial key agreement is formed by two protocols called IKA.1 and IKA.2 (they were referred to as GDH.2 and GDH.3, respectively.) The first IKA.1 is simple and straightforward. It consists of upflow and downflow stages. The purpose of the upflow stage is to collect contributions from all group members, one per round. In the second stage M_n broadcasts the intermediate values to all group members, so every member can calculate the group key .In order to minimize the amount of computation performed by each group member IKA.2 is constructed. IKA.2 consists of four stages .In the first stage, author collect contribution from all group members similar to the upflow sage in IKA.1. After processing the upflow message M_{n-1} obtains $\alpha^{\pi N_p | p[1,n-1]}$ and broadcasts this value in second stage to all other participants. At this time, every $M_i (i \neq n)$ factors out its own exponent and forwards the result to M_n. In the final stage, M_n collects all inputs from the previous stage, raises every one of them to the power N_n and broadcasts the resulting n-1 values to the rest of the group. Initial group key agreement is only a part, although a major one, of the protocol suite needed to support secure communications in dynamic groups. Here we discuss other auxiliary group key operations. The security property crucial to all AKA operations is key independence .The AKA operations involving single group members are member addition and member exclusion. Subgroup Operations are group addition and group exclusion. Group addition, in turn, has two variants: mass join and group fusion. Similarly, subgroup exclusion can also be thought of as: mass leave, group division and group fission. Another group key operation is group key refresh. The AKA operations take advantage of the keying information collected in gathering phase of the most recent IKA protocol run. This information is incrementally updated and redistributed to the new incamation of the group. In particularly, any member who caches the most recent message of the final broadcast round can initiate an AKA operation. Any member can take over the role of group controller at no cost and whenever the situation requires it. Here we only give the figure of the member addition protocol.

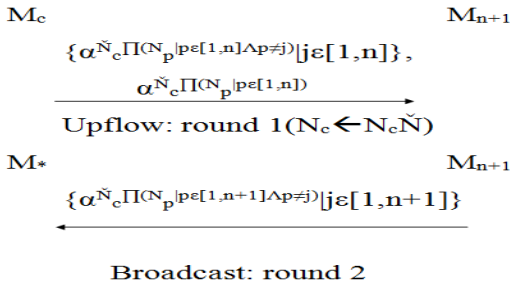

Figure 1 AKA member addition

IV. RSA ALGORTIHM

RSA[6] is an algorithm for public key cryptography which is based on the presumed difficulty of factoring large integers. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978 . A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors need to be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods , when the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem .

1) Encryption

Sender transmits her public key (*n*,*e*)to receiver and keeps the private key secret.Receiver then wishes to send message M to Sender. He first turns M into an integer0< m<n, such that by using an agreed-upon reversible protocol known as a padding scheme . He then computes the ciphertext c corresponding to :

$$c=m^e \pmod n$$

where n=p*q, modulus for bot the public and private keys. p and q are prime numbers. E is an integer such that 1<e<f(n), and e and f(n) are coprime.This can be done quickly using the method of exponentiation by squaring . Receiver then transmits c to Sender. Note that, at least nine values of m could yield a cipher text c equal to m,but this is very unlikely to occur in practice.

2) Decryption

Sender can recover m from c by using her private key exponent d via computing

$$m=c^d \pmod n$$

where d is privete key exponent such that d*e=1(mod f(n)). Given m , he can recover the original message M by reversing the padding scheme . The above decryption procedure works because:

$$m=(m^e)^d \pmod n = m^{ed} \pmod n.$$

Now, since e*d=1+k * f (n), $m^{ed}=m^{1+k*f(n)} = m*(m^k)^{f(n)} = m \pmod n$. The last congruence directly follows from Euler's theorem when *m* is relatively prime to *n*. By using the Chinese remainder theorem it can be shown that the equations hold for all *m*. This shows that the original message is retrieved:

$$c^d=m \pmod n.$$

V. PROPOSED WORK

Generally authors imply security on all the nodes of the network. But this causes wastage of time and cost. The author will first find out the shortest path between source and destinitions nodes and then imply the security in multicast routing. This prevents wastage of time and cost. The keys are exchanged with the help of GDH(Group Diffie-Hellman Algorithm with n-parties) and the Encryption and Decryption of data is done with the help of RSA Algorithm. This proposed scheme will improve the performance of the network such as delay and packet delivery ratio.

A. Flow Chart of Proposed Algorithm

Here the Flow chart of the proposed work is presented. As we know the flow chart is the graphical representation of the algorithmic work.

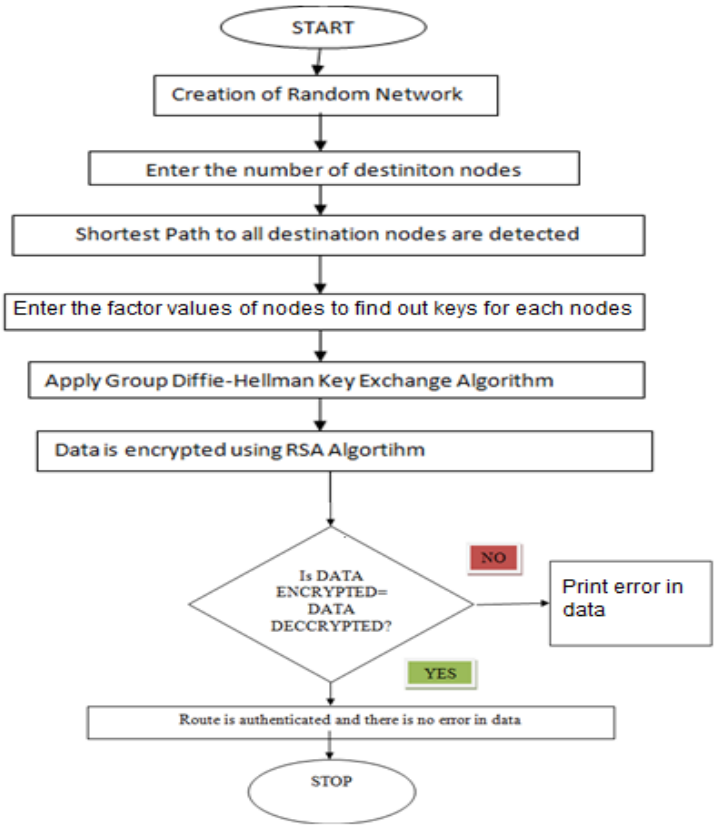

Figure 2 Flowchart of Proposed Work

VI. Conclusion

Multicasting is used when the same message or the same stream of data must be forwarded to multiple destinations. . Multicasting is an efficient data transmission method to support group-oriented communications in one-to-many or many-to-many applications such as audio/video conferencing, collaborative works, and so on. In MANETs, the most challenging issue in multicast routing is to effectively handle the attacks and provide authenticity of data. The proposed work is to Authenticate the modification attack if any persists in dedicated route from source to destination node. The proposed work showed that secured multicast routing protocol may improve network performance in terms of delay, throughput, reliability or lifetime. The implementation is performed in java and analysis is presented using a snapshots and graph.

Case I: If there is no intermediate node in between one to many communication. Then there is no way that the key exchanged between the two nodes gets intended and the data transfer is secure.

Case II: if there are some intermediate node in between one to many communications i.e along the path between the source and the different destination nodes and if some malicious node intrudes the key and change it and then forwards it to the destined nodes waiting for the key to be shared, the destined nodes will not be able to know whether the key coming to be shared is either intruded or not and take it as a key that is not infected from any malicious node(intruder) . The data then decrypted will not be the same as sent.

VII. Future Work

The proposed system can be enhanced in future by other researchers in the following ways

- If Case II occurs then author needs to detect the malicious node along the whole path and to make the path secure so that data can be transferred securely over the path without any intrusion.
- Secondly , it can be enhanced for multiple source node. That is to send data from different sources to different destinitions.

REFERENCES

[1] Andrea Goldsmith, "*Wireless Communications*", Cambridge University Press, August 2005.

[2] Elizabeth M. Royer And Chai-Keong Toh, "*A Review Of Current Routing Protocols For Ad-Hoc Mobile Wireless Networks*", IEEE Personal Communications, April 1999.

[3] Jon Kleinberg, Eva Tardos , "*Algorithm Design*", Pearson Education India, 2006.

[4] Emmanuel Bresson,Olivier Chevassut and David Pointcheval, "*Dynamic Group Diffie-Hellman Key Exchange under Standard Assumptions*", LNCS 2332, pp. 321–336, 2002.

[5] D.Suganyadevi And Dr.G.Padmavathi, "*Secure Multicast Key Distribution For Mobile Adhoc Networks*", IJCSIS,Vol. 7, No. 2, 2010.

[6] Satyendra Nath Mandal, Kumarjit Banerjee, Biswajit Maiti and J. Palchaudhury, "*Modified Trail division for Implementation of RSA Algorithm with Large Integers*", Int. J. Advanced Networking and Applications Volume: 01, Issue: 04, Pages: 210-216 , 2009.

