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: A Review

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 key and data transmission over the network. Security will be provide in two way: one for key exchange by GDH for n parties and another for data security by RSA. Security is done after Distributed Bellman Ford applied for finding shortest path among source and various destination nodes.

Keywords— MANET, DBF, GDH, RSA, Multicasting

I. INTRODUCTION

Wireless communication technology have been developed with two primary models one is fix infrastructure based model in which much of the nodes are mobile and connected through fixed backbone nodes using wireless medium. Another model is Mobile Ad-hoc network. Mobile Ad-Hoc Networks (MANETs) are comprised of mobile nodes (MNs) that are self-organizing and cooperative to ensure efficient and accurate packet routing between nodes. There are no specific routers, servers, access points for MANETs. Because of its fast and easy of deployment, robustness, and low cost. Typical MANETs applications could be find in the following areas like Military applications battlefield), Search and rescue operations, Temporary networks within meeting rooms, airports, and other wearable computers etc. Design issue for developing a routing protocol for wireless environment with mobility is very different and more complex than those for wired network with static nodes [1]. Main problem in mobile ad hoc network are Limited bandwidth and frequently change in the topology. Although there are lots of routing protocols that can be used for multicast communication within the Mobile Ad hoc networks, it observes that any one protocol cannot fit in all the different scenarios, different topologies and traffic patterns of Mobile Ad-Hoc Networks applications.

A. *Multicasting*

Multicasting plays an important role in typical applications of ad hoc wireless networks, namely emergency, search and rescue operations and military communication[4]. In such an environment, nodes form groups to carry out certain tasks that require point-to-multipoint and multipoint-to-multipoint voice and data communication. The arbitrary movement of nodes changes the topology dynamically in an unpredictable manner. The mobility of nodes, with the constraints of power source and bandwidth, make multicast routing very challenging. The use of multicasting within MANETs has many benefits. It can decrease the cost of wireless communication and increase the efficiency and throughput of the wireless link between two nodes whenever we are sending multiple copies of the same messages by accomplishment the inherent broadcasting properties of wireless transmission. In place of sending same data through multiple unicasts, multicasting decrease channel capacity consumption, sender nodes and routers processing, energy utilization , and data delivery delay, which are deliberate important for MANETs. If the mobile nodes in the MANET move too quickly, they have to repair to broadcast to achieve node to node communication. Every routing protocol has its advantages and disadvantages, and aims at a specific application. Finally, the expected standard for routing protocols in the Mobile Ad-Hoc Networks is very likely to combine some of the most competitory schemes. The major issues in designing are as follows:

- ***Efficiency:*** A multicast protocol should make a minimum number of transmissions to deliver a data packet to all group members.
- ***Control Overhead:*** The scarce bandwidth availability in ad hoc wireless networks demands minimum control overhead for multicast session.
- ***Quality Of Service:*** QoS support is essential in multicast routing because, in most cases, the data transferred in multicast session is time sensitive.
- ***Scalability:*** The multicast routing protocol should be able to scale for a network with a large number of nodes.
- ***Security:*** Authentication of session members and prevention of non members from gaining unauthorized information plays a major role in military communication.

B. *Security in MANETs*

Security in a MANET is an essential component for basic network functions like packet forwarding and routing[2]. Unlike conventional networks, the ad hoc networks carry out basic support functions like - packet forwarding, routing, and network management all of the available nodes without the support of dedicated nodes and also the data travels through the open medium. As opposed to dedicated nodes of a wired network, the nodes of an ad hoc network cannot be trusted for the correct execution of critical network functions. Due to the lack of a priori trust, classical network security mechanisms based on authentication and access control cannot cope with selfishness and cooperative security schemes seem to offer the only reasonable solution.

1. *Security Goals*

Security services include the functionality required to provide a secure networking environment[2][3]. The main security services can be summarized as follows:

- ***Authentication:*** This service verifies a user's identity and assures the recipient that the message is from the source that it claims to be from. Firstly, at the time of communication initiation, the service assures that the two parties are authentic, that each is the entity it claims to be. Secondly, it must assure that a third party does not interfere by impersonating one of the two legitimate parties for the purpose of authorized transmission and reception. Authentication can be provided using encryption along with cryptographic hash functions, digital signatures and certificates.
- ***Confidentiality:*** This service ensures that the data/information transmitted over the network is not disclosed to unauthorized users. Confidentiality can be achieved by using different encryption techniques such as only legitimate users can analyze and understand the transmission.
- ***Integrity:*** The function of integrity control is to assure that the data is received in verbatim as sent by authorized party. The data received contains no modification, insertion or deletion.
- ***Access Control:*** This service limits and controls the access of such a resource, which can be a host system or an application.
- ***Availability:*** This involves making the network services or resources available to the legitimate users. It ensures the survivability of the network despite malicious incidences.

C. *Multicasting Routing Protocols*

Multicasting routing protocols have emerged as one of the most focused areas in the field of MANETs. There are three basic categories of multicast methods [4] in MANETs:

1. A basic method is to simply flood the network. Every node receiving a message floods it to a list of neighbors. Flooding a network acts like a chain reaction that can result in exponential growth.

2. The proactive approach pre-computes paths to all possible destinations and stores this informa tion in the routing table. To maintain an up-todate database, routing information is periodically distributed through the network.

3. The final method is to create paths to other nodes on demand. The idea is based on a query response mechanism or reactive multicast. In the query phase, a node explores the environment. Once the query reaches the destination the response phase starts and establishes the path.

Recently, many multicast routing protocols have been newly proposed to perform multicasting in MANETs. These include ad-hoc multicast routing protocol utilizing increasing Id numbers (AMRIS) [11], multicast ad-hoc on-demand vector (MAODV) [12], core assisted mesh protocol (CAMP) [13], lightweight adaptive multicast (LAM) [14], location guided tree (LGT) [15], on-demand multicast routing protocol (ODMRP) [16], forwarding group multicast protocol (FGMP) [17], ad-hoc multicast routing (AMRoute) [18], multicast core extraction distributed ad-hoc routing (MCEDAR)[19] and differential destination multicast (DDM) [20]. Most of these multicast routing protocols are primarily based on flavors of distance-vector or link-state routing plus additional functionalities to assist the routing operations in particular ways. The goals of all these protocols include minimizing control overhead, minimizing processing overhead, maximizing multi-hop routing capability, maintaining dynamic topology and preventing loops in the networks etc. However, many multicast routing protocols do not perform well in MANETs because in a highly dynamic environment, nodes move arbitrarily, thus network topology changes frequently and unpredictably. Moreover, bandwidth and battery power are limited. These constraints in combination with the dynamic network topology make multicasting routing protocol designing for MANETs extremely challenging.

II. SHORTEST PATH PROBLEM

In graph theory, the shortest path problem is the problem of finding a path between two vertices (or nodes) in a graph such that the sum of the weights of its constituent edges is minimized[6]. This is analogous to the problem of finding the shortest path between two intersections on a road map: the graph's vertices correspond to intersections and the edges correspond to road segments, each weighted by the length of its road segment. In particular we are interested in the single-source shortest paths problem over directed graphs with no negative edge weights. . In general a graph G = (V, E) consists of a set of vertices V, and a set of edges E is belongs to V_1*V, along with an edge weight function w : E->N. A path p = [v_0, v_1, . . . , v_k] has path weight w(p) = w(v_0, v_1) + w(v_1, v_2) + . . . + w(v_{k1}, v_k). A zero-length path p = [v_0] has weight 0. The shortest path weight d(u, v) from vertex u to v is min({w(p) | p εP(u, v)}) where P(u, v) is the set of all paths p = [u, . . . , v] in the graph, or ∞ if there are no such paths. A particular path p 2 P(u, v) is a (not necessarily unique) shortest path if w(p) = d(u, v)[10].

A. *Distributed Bellman Ford*

In network routing, each vertex in the graph corresponds to a router and each edge corresponds to a communication link between routers[10]. If each router in a network of size N stores the complete adjacency matrix A, the algorithm's per-router memory requirements are O(N_2), leading to a scalability problem in large networks. Routing protocols based on Dijkstra's algorithm, such as OSPF, are typically restricted to small networks due to this scalability issue. However, protocols based on Bellman-Ford can use a distributed variant of the algorithm in which the requirements on each individual router scale as O(N), allowing larger networks to be handled efficiently, with the tradeoff of slowing the algorithm's execution by adding communication delays. The distributed Bellman-Ford algorithm (DBF) is based on the observation that the original BF algorithm can be written as in pseudocode, and that the iteration on step 5 can be executed in parallel with every router processing the v corresponding to itself. In this case, router v will only need to know the element x[v], plus x[u] and w(u, v) for each router u to which it has an edge. These edges correspond to network links, so v can easily determine these values by communicating directly with each u over the network. The amount of data stored and processed by v will scale with the number of routers to which it has an edge, so it is bounded by O(N). As a final modification, the loop on step 4 is removed: every router repeats step5–8 forever and asynchronously. Although it is hard to tell how long the algorithm will now take to reach the solution, it will eventually converge to the same solution as the original Bellman-Ford algorithm. Bertsekas gives a proof of convergence for the asynchronous DBF shortest-paths algorithm, while Sobrinho gives a proof for an asynchronous message-passing path vector protocol based on DBF that is generalised to certain routing algebras.

Steps For Distributed Bellman-Ford Algorithm are:

```
Step 1: for each vertex v ϵ V[G]
Step 2: do x[v] ← ∞
Step 3: x[d] ← 0
Step 4: for i ←1 to [V[G]]-1
Step 5: do for each vertex v ϵ V[G]
Step 6: do for each vertex u ϵ V[G] where (u, v) ϵ E[G]
Step 7: do if x[v] > x[u] + w(u, v)
Step 8: then x[v]←x[u] + w(u, v)
```

III. KEY EXCHANGE PROBLEM

The key exchange problem is how to exchange whatever keys or other information are needed so that no one else can obtain a copy. Traditionally, this required trusted couriers, diplomatic bags, or some other secure channel. With the advent of public key / private key cipher algorithms, the encrypting key could be made public, since (at least for high quality algorithms) no one without the decrypting key could decrypt the message. There are several methods given in key management approaches that can be employed to perform this operation, all requiring varying amounts of initial configuration, communication and computation. According to this approach, the key management responsibility is shared among a set of trusted certification servers called the CAs. Each CA has a public/private key pair, with its public key known to every node, and signs certificates binding public keys to nodes after verifying their authenticity secretly[7].

A. *Group Diffie-Hellman For n Parties Protocol*

GDH is a contributory key agreement protocol which is essentially an extension of the two party Diffie-Hellman protocol[8]. 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 os 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 . 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:

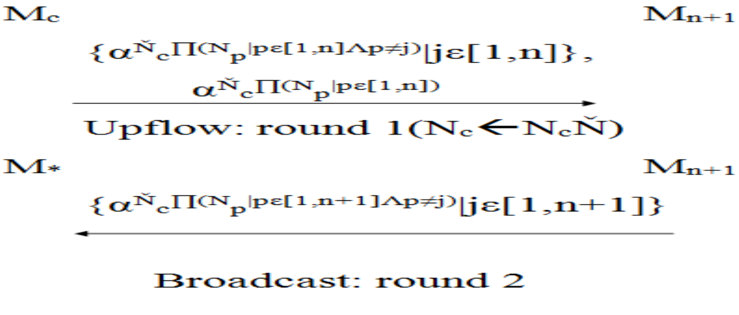
M_c
M_{n+1}
$\{\alpha^{\check{N}_c \Pi(N_p | p\varepsilon[1,n] \wedge p\neq j)} | j\varepsilon[1,n]\}$,
$\alpha^{\check{N}_c \Pi(N_p | p\varepsilon[1,n])}$
Upflow: round 1($N_c \leftarrow N_c\check{N}$)
M_*
M_{n+1}
$\{\alpha^{\check{N}_c \Pi(N_p | p\varepsilon[1,n+1] \wedge p\neq j)} | j\varepsilon[1,n+1]\}$
Broadcast: round 2

Figure1 AKA member addition

IV. RSA ALGORITHM

Encipherment or message encryption is the science and art of transforming a message into a disguised version which no unauthorized person can read, but which can be recovered in its original form by an intended recipient[9]. In the parlance of cryptography, the original message is called plaintext and the secret version of the message is called ciphertext. The plaintext is converted into ciphertext by the process of encryption, that is, by the use of certain algorithms or functions. The reverse process is called decryption. The process of encryption and decryption are governed by keys, which are small amount of information used by the cryptographic algorithms. There are two types of encryption techniques:

symmetric key and asymmetric key (or public key). Symmetric key cryptosystem uses the same key (the secret key) for encryption and decryption of a message, where as asymmetric key cryptosystems use one key (the public key) to encrypt a message and another key (the private key) to decrypt it. Public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used for decryption purpose. Even if attacker comprises a public key, it is virtually impossible to deduce the private key. Symmetric key algorithms are usually faster to execute electronically than the asymmetric key algorithms. RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described the algorithm in 1977. Clifford Cocks, an English mathematician, had developed an equivalent system in 1973, but it wasn't declassified until 1997. A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

V. CONCLUSION AND FUTURE WORK

We conclude that secured multicast routing protocol may improve network performance in terms of delay, throughput, reliability or lifetime. It will provide security in two ways; one for key security and another for data security. If there are some attacker 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. The proposed system can be enhanced in future by other researchers to detect the attacker 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] Mohit Kumar And Rashmi Mishra,"*An Overview Of Manet: History, Challenges And Applications*" , ISSN : 0976-5166 Vol. 3 No. 1 Feb-Mar 2012.

[3] Priyanka Goyal,Vinti Parmar,Rahul Rishi, "*Manet: Vulnerabilities, Challenges, Attacks, Application*", IJCEM .Vol.11.January2011.

[4] Abdussalam Nuri Baryun, And Khalid Al-Begain , "*A Design Approach For Manet Multicast Protocols*", ISBN: 978-1-902560-19-9,PGNET,2008.

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

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

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

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

[9] 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.

[10] Philip J. Taylor , "*Specification of policy languages for network routing protocols in the Bellman-Ford family*", University of Cambridge, Computer Laboratory, King's College, September 2011.

[11] C.W. Wu, Y.C. Tay, C.K. Toh, "*Ad-hoc Multicast Routing Protocol Utilizing Increasing Id-numbers (AMRIS) Functional Specification*," Internet draft, November 1998.

[12] E.M. Royer, C.E. Perkins, "*Multicast operation of the ad-hoc on-demand distance-vector routing protocol*", ACM MOBICOM (1999) 207–218. August.

[13] L. Ji, M.S. Corson, "*A lightweight adaptive multicast algorithm", *GLOBECOM (1998) 1036–1042.

[14] J.J. Garcia-Luna-Aceves, E.L. Madruga, "*The core-assisted mesh protocol"*, IEEE JSAC (1999) 1380–1394. August.

[15] K. Chen, K. Nahrstedt, " *Effective location-guided tree construction algorithms for small group multicast in MANET*", Proceedings of the INFOCOM (2002) 1180–1189.

[16] M. Gerla, S.J. Lee, W. Su, " *On-Demand Multicast Routing Protocol (ODMRP) for Ad-hoc Networks*", Internet draft, draft-ietf-manet-odmrp-02.txt, 2000.

[17] C.C. Chiang, M. Gerla, L. Zhang, "*Forwarding group multicast protocol (FGMP) for multi-hop"*, Mobile Wireless Networks, AJ. Cluster Comp, Special Issue on Mobile Computing, vol. 1 (2), 1998, pp. 187–196.

[18] E. Bommaiah et al., "*AMRoute: Ad-hoc Multicast Routing Protocol"*, Internet draft, August 1998.

[19] P. Sinha, R. Sivakumar, V. Bharghavan, " *MCEDAR: multicast core-extraction distributed ad-hoc routing"*, IEEE Wireless Communications and Networking Conference, September 1999, pp. 1313–1317.

[20] L. Ji, M.S. Corson, "*Differential destination multicast-a MANET multicast routing protocol for small groups"*, Proc. INFOCOM (2001) 1192–1201.