International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 5 (May 2014), PP.07-11

Efficient Geographic Multicast Protocol for Mobile Adhoc Networks

Ramesh.K Deosur Umesh
Associate Professor, Dept. of Computer Science Research Scholar, Dept. of Computer Science
Karnataka State Women's University Bijapur, India Karnataka University Dharwad, India

Abstract:- Multicasting is the transmission of packets to a group of zero or more hosts identified by a single destination address. Multicasting is intended for group-oriented computing. Many techniques' are used for transmission of data. Different techniques use different multicasting protocols. Conventional multicast protocols generally do not have good scalability due to the overhead incurred, for route searching, group membership management, and creation and maintenance of the tree/mesh structure over the dynamic MANET. For MANET unicast routing, geographic routing protocols have been proposed in recent years for more scalable. In this paper, proposed scheme is based on identity-based and threshold three level key management scheme which adopts Elliptic Curve Cryptography (ECC). It is well known that ECC is appropriate for such nodes due to its smaller keys and its higher security levels. The pairing technology provides authentication and confidentiality with reduced communication overhead and computational cost. This scheme which combined the identity-based and threshold cryptography can satisfy the secure requirements and provides efficiency in geographic multicasting of MANET.

Keywords:- Efficiency, Muticast Routing, Security

I. INTRODUCTION

Conventional MANET multicast protocols can be described into two main categories, tree-based and mesh based. However, due to the constant movement as well as frequent network joining and leaving from individual nodes, it is very difficult to maintain the tree structure using these conventional tree-based protocols (e.g., MAODV, AMRIS, MZRP, and MZR). The mesh-based protocols (e.g., FGMP, Co re-Assisted Mesh protocol, ODMR) are proposed to enhance the robustness with the use of redundant paths between the source and the destination pairs.

Conventional multicast protocols generally do not have good scalability due to the overhead incurred for route searching, group membership management, and creation and maintenance of the tree/mesh structure over the dynamic MANET. For MANET unicast routing, geographic routing protocols have been proposed in recent years for more scalable and robust packet transmissions. The existing geographic routing protocols generally assume mobile nodes are aware of their own positions through certain positioning system, and a source can obtain the destination position through some type of location service an intermediate node makes its forwarding decisions based on the destination position inserted in the packet header by the source and the positions of its one-hop neighbors learned from the periodic beaconing of the neighbors.

By default, the packets are greedily forwarded to the neighbor that allows for the greatest geographic progress to the destination. When no such a neighbor exists, perimeter forwarding is used to recover from the local void, where a packet traverses the face of the planarized local topology sub-graph by applying the right-hand rule until the greedy forwarding can be resumed. Similarly, to reduce the topology maintenance overhead and support more reliable multicasting, an option is to make use of the position information to guide multicast routing. However, there are many challenges in implementing an efficient and scalable geographic multicast scheme in MANET. For example, in unicast geographic routing, the destination position is carried in the packet header to guide the packet forwarding, while in multicast routing, the destination is a group of members. A straight-forward way to extend the geography-based transmission from unicast to multicast is to put the addresses and positions of all the members into the packet header, however, the header overhead will increase significantly as the group size increases, which constrains the application of geographic multicasting only to a small group. Besides requiring efficient packet forwarding, a scalable geographic multicast protocol also needs to efficiently manage the membership of a possibly large group, obtain the positions of the members and build routing paths to reach the members distributed in a possibly large network terrain. The existing small-group-based geographic multicast protocols normally address only part of these problems.

II. STATEMENT OF PROBLEM

This project simulates a new efficient geographic multicast protocol for mobile ad-hoc networks which solve the problem in group communication when the network size is large by dividing the network into virtual zones.

This project also contains elliptical curvy cryptography (ECC) algorithm which is cryptography algorithm for security.

III. OBJECTIVES OF THE PROJECT

1) Design and implementation of the efficient geographic multicast protocol for mobile ad-hoc networks to perform group communication.
2) Design and implementation of elliptical curvy cryptography (ECC) algorithm which is cryptography algorithm for security.

IV. LITERATURE SURVEY

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

The existing geographic routing protocols generally assume mobile nodes are aware of their own positions through certain positioning system (e.g., GPS), and a source can obtain the destination position through some type of location service. In an intermediate node makes its forwarding decisions based on the destination position inserted in the packet header by the source and the positions of its one-hop neighbors learned from the periodic beaconing of the neighbors. By default, the packets are greedily forwarded to the neighbor that allows for the greatest geographic progress to the destination. When no such a neighbor exists, perimeter forwarding is used to recover from the local void, where a packet traverses the face of the planarized local topology sub graph by applying the right-hand rule until the greedy forwarding can be resumed.

ODMRP are proposed to enhance the robustness with the use of redundant paths between the source and the destination pair’s scalability due to the overhead incurred for route searching, group membership management, and creation and maintenance of the tree/mesh structure over the dynamic MANET.

For MANET unicast routing, geographic routing protocols have been proposed in recent years for more scalable and robust packet transmissions we proposed an efficient and robust geographic multicast protocol for MANET. In this paper, we further introduce zone-supported geographic forwarding to reduce the routing failure, and provide mechanism to handle zone partitioning. In addition, we introduce a path optimization process to handle multiple paths, and provide a detailed cost analysis to demonstrate the scalability of the proposed routing scheme.

4.1 A Scalable Multicasting with Group Mobility Support in Mobile Ad Hoc Networks

In mobile ad hoc networks, an application scenario requires mostly collaborative mobility behavior. The key problem of those applications is scalability with regard to the number of multicast members as well as the number of the multicast group. To enhance scalability with group mobility, we have proposed a multicast protocol based on a new framework for hierarchical multicasting that is suitable for the group mobility model in MANET. The key design goal of this protocol is to solve the problem of reflecting the node’s mobility in the overlay multicast tree, the efficient data delivery within the sub-group with group mobility support, and the scalability problem for the large multicast group size. The results obtained through simulations show that our approach supports scalability and efficient data transmission utilizing the characteristic of group mobility.

4.2 Selective Destination Multicasting over Mobile Ad Hoc Networks

Mobile Ad-hoc network (MANET) is a self-configuring wireless system, which connect the mobile devices without use of any fixed network infrastructure or centralized coordination. Group communications are the major role in MANET communication which is efficiently implemented by Multicasting. But, there are big challenges to implement efficient and reliable multicasting due to difficult in group membership management and multicast packet delivery over a dynamic MANET. In recent years various multicast protocols have been designed distinct for MANETs. All these multicast protocols follow the conventional multicast approaches. We propose a Selective Destination Geographic Multicast Protocol (SDGMP). It uses a virtual zone based structure to implement reliable and efficient group membership management. Position information is used to track individual nodes location. The virtual zone is divided into cluster to attain more efficient group management and multi cast packet delivery. To further improve the efficiency, SDGMP introduces the concept of selective destination multicasting for efficient packet delivery. The efficiency of the SDGMP is evaluated through simulations and performance evaluation.

4.3 Efficient and Robust Multicast Routing in Mobile Ad Hoc Networks

We present the protocol for unified multicasting through announcements (PUMA) in ad-hoc networks, which establishes and maintains a shared mesh for each multicast group, without requiring a unicast routing protocol or the pre assignment of cores to groups. PUMA achieves a high data delivery ratio with very limited control overhead, which is almost constant for a wide range of network conditions. Using simulations in Qualnet 3.5, we compare PUMA with ODMRP and MAODV, which are representatives of mesh-based and tree-based multicast routing in ad hoc networks. The results from a wide range of scenarios of varying mobility, group members, number of senders, traffic load, and number of multicast groups show that PUMA attains higher packet delivery ratios than ODMRP and MAODV, while incurring far less control overhead.

V. PROPOSED SYSTEM

ODMRP are proposed to enhance the robustness with the use of redundant paths between the source and the destination pair's scalability due to the overhead incurred for route searching, group membership management, and creation and maintenance of the tree/mesh structure over the dynamic MANET.

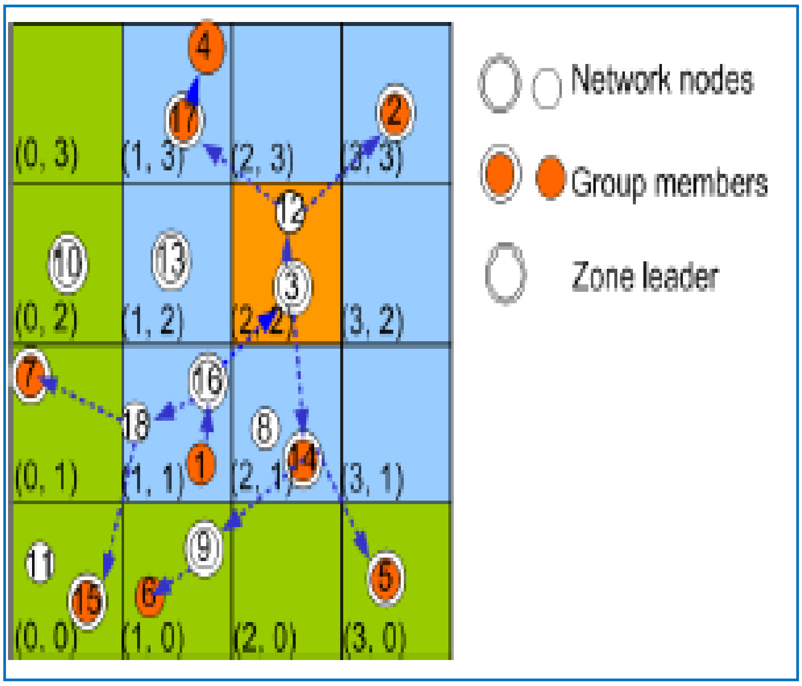
For MANET unicast routing, geographic routing protocols have been proposed in recent years for more scalable and robust packet transmissions we proposed an efficient and robust geographic multicast protocol for MANET. In this paper, we further introduce zone-supported geographic forwarding to reduce the routing failure, and provide mechanism to handle zone partitioning. In addition, we introduce a path optimization process to handle multiple paths, and provide a detailed cost analysis to demonstrate the scalability of the proposed routing scheme.

VI. SYSTEM ARCHITECTURE

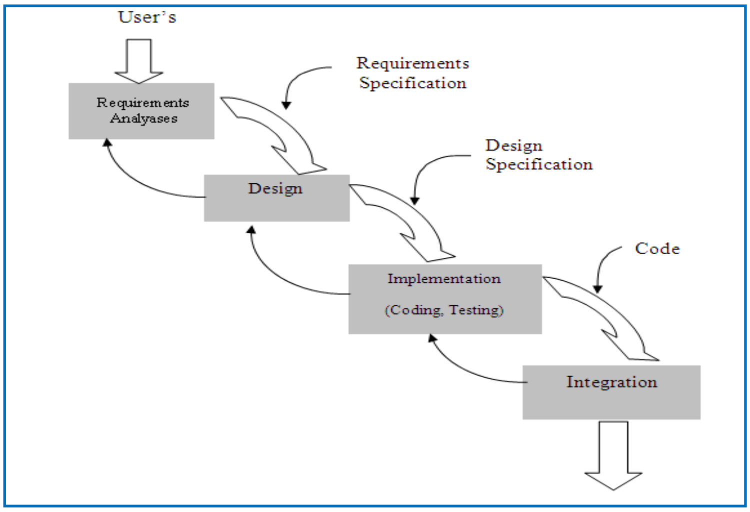
System architecture is the conceptual design that defines the structure and behavior of a system. An architecture description is a formal description of a system, organized in a way that supports reasoning about the structural properties of the system. It defines the system components or building blocks and provides a plan from which products can be procured, and systems developed, that will work together to implement the overall system.

Network: Here the networks are divided into different zones as shown in the figure. These zones are virtual zones which help in group communication with security.

Zones: When network is divided into zones a leader is elected in every zone to maintain the group membership management and details of the local group members



VII. PROJECT LIFE CYCLE



As shown in the above figure user send the request for transmission the with respect to the requirement specification designing is done and then this complete process is integrated and gives back as result as required.

VIII. OUTPUT DESIGN

A quality output is one, which meets the requirements of the end user and presents the information clearly. In any system results of processing are communicated to the users and to other system through outputs. In output design it is determined how the information is to be displaced for immediate need and also the hard copy output. It is the most important and direct source information to the user. Efficient and intelligent output design improves the system's relationship to help user decision-making.

1. Designing computer output should proceed in an organized, well thought out manner; the right output must be developed while ensuring that each output element is designed so that people will find the system can use easily and effectively. When analysis design computer output, they should Identify the specific output that is needed to meet the requirements.
2. Select methods for presenting information.
3. Create document, report, or other formats that contain information produced by the system.

The output form of an information system should accomplish one or more of the following objectives. Convey information about past activities, current status or projections of the Future Signal important events, opportunities, problems, or warnings. Trigger an action. Confirm an action.

IX. CONCLUSION

In summary, the proposed scheme is based on identity-based and threshold three level key management scheme which adopts Elliptic Curve Cryptography (ECC) in this paper. It is well known that ECC is appropriate for such nodes due to its smaller keys and its higher security levels. (t, n)threshold secret sharing algorithm has been improved to resist adversary's attack and ensure availability of network services, such as key generation and key distribution. The pairing technology provides authentication and confidentiality with reduced communication overhead and computational cost. Our scheme which combined the identity-based and threshold cryptography can satisfy the secure requirements of MANET.

REFERENCES

[1] HU Rong-lei, LIU Jian-wei, ZHANG Qishan.“Cluster-based key management scheme for adhocnetworks”.Journal on Communications, china.Vol.29 No.10. October 2008. pp.223-228.

[2] H. Luo, J. Kong, P. Zerfos, S. Lu, and L. Zhang,“URSA: Ubiquitous and Robust Access Control for Mobile Ad Hoc Networks,“ IEEE/ACM Transactions on Networking ,Decembe2004, pp. 1049-1063

[3] W. Du, J. Deng, Y. S. Han, P. Varshney, J.Katz, and A. Khalili, “A Patrwise Ke Redistributions Scheme for Wireless Sensor Networks,” ACM Transactions on Information and System Security (TISSEC), 2005 , pp. 228-258.

[4] D. Wallner, E. Harder, and R. Agee, “KeyManagement for Multicast: Issues and Architectures”, RFC 2627, 1999.

[5] A. Ballardie, “Scalable Multicast KeyDistribution”, RFC1949, 1996.

[6] N. Asokan and P. Ginzboorg, “Key Agreementin ad hoc networks”, Elsevier Journal of Computer Communications.Vol. 23, pp. 1627– 1637, 2000.

[7] A.Shamir: “Identity based cryptosystems andsignature schemes.” Advances in Cryptology–Proceedings of Crypto’84 pp. 47-53, 1984.

[8] A.Fiat, A.Shamir: How to Prove Yourself:practical Solutions to Identification andSignature Problems.

[9] L.Guilou, J-J. Quisquater: A “Paradoxical”identity based Signature Scheme Resulting From Zero-Knowledge. Advances in Cryptology Crypto’88, LNCS 0403, Springer(1988) 216-231.

[10] D. Boneh and M.Franklin: Identity-basedEncryption from the Weil Pairing. Proc CRYPTO’01(2001) 213-229.

[11] D. Boneh and M.Franklin: Identity based Encryption from the Weil Pairing. SIAMJ. Computing, vol. 32, no. 3(2003) 586-615.

[12] B.Lynn: Authenticated Identity-based Encryption. Available at http://eprint.iacr.org (2002).

[13] WATERS B R: Efficient identity-base encryption without random oracles[R].Cryptology ePrint Archive, Report 2004/180,http://epring.iacr.org (2004).

[14] Javier Herranz: Identity-based ring signatures from RSA. Theoretical Computer Science 389(2007) 100-117.

[15] J.Pan, L.Cai, X.Shen, J.W.Mark: Identity basedsecure collaboration in wireless Ad hoc networks. Computer Network 51(3)(2007)853-865.

[16] G.Frey, M.Muller, H.riick: The Tate pairingand the discrete logarithm applied to elliptic curve.

[17] A.Menezes, T.Okamoto, and S.VanstoneL: Reducing elliptic curve logarithms to logarithms in a finite field.

[18] Shamir.A: How to share a secret. Communications of the ACM vol.22 no.11 (1979) 612-613.

[19] T.Pedersen: Non-interactive and information theoretic secure verifiable secret sharing. In J.Feigenbaum, editor, Advances in Cryptology- Crypto’91, the 11th Annual International Cryptology Conference, Santa Barbara, CA USA, August 11-15, 1991.