Volume : 1 | Issue : 3 | March 2012 ISSN - 2250-1991

Research Paper Information Technology

A Secure Group Communication Architecture For a Mobile Communication Networks

* Ms. V. Sunitha Reddy ** Mr. C.S. Jayanthi Prasad

*, ** Associate Professor, Jaya Prakash Narayan College of Engineering, Dharmapur, Mahabubnagar, Andhra Pradesh

ABSTRACT

Group communications are important in Mobile Ad hoc Networks (MANET). Multicast is an efficient method for implementing group communications. However, it is challenging to implement efficient and scalable multicast in MANET due to the difficulty in group membership management and multicast packet forwarding over a dynamic topology. We propose a novel Efficient Geographic Multicast Protocol (EGMP). EGMP uses a virtual-zone-based structure to implement scalable and efficient group membership management. A network-wide zone-based bi-directional tree is constructed to achieve more efficient membership management and multicast delivery. The position information is used to guide the zone structure building, multicast tree construction and multicast packet forwarding, which efficiently reduces the overhead for route searching and tree structure maintenance. Several strategies have been proposed to further improve the efficiency of the protocol, for example, introducing the concept of zone depth for building an optimal tree structure and integrating the location search of group members with the hierarchical group membership management. Finally, we design a scheme to handle empty zone problem faced by most routing protocols using a zone structure. The scalability and the efficiency of EGMP are evaluated through simulations and quantitative analysis. Our simulation results demonstrate that EGMP has high packet delivery ratio, and low control overhead and multicast group joining delay under all test scenarios, and is scalable to both group size and network size. Compared to Scalable Position-Based Multicast (SPBM), EGMP has significantly lower control overhead, data transmission overhead, and multicast group joining delay.

Keywords : Routing Table, wireless networks, mobile ad hoc networks, Efficient Geographic Multicast Protocol (EGMP), Multicasting

Literature Review:

Security is a major concern for protected communication between mobile nodes in a hostile environment. In hostile environments adversaries can bunch active and passive attacks against intercept able routing in embed in routing message and data packets. In this paper, we focus on fundamental security attacks in Mobile ad hoc networks. MANET has no clear line of defense, so, it is accessible to both legitimate network users and malicious attackers. In the presence of malicious nodes, one of the main challenges in MANET is to design the robust security solution that can protect MANET from various routing attacks. However, these solution are not suitable for MANET resource constraints, i.e., limited bandwidth and battery power, because they introduce heavy traffic load to exchange and verifying keys. MANET can operate in isolation or in coordination with a wired infrastructure, often through a gateway node participating in both networks for traffic relay. This flexibility, along with their self organizing capabilities, are some of MANET's biggest strengths, as well as their biggest security weaknesses. In this paper different routing attacks, such as active (flooding, black hole, spoofing, wormhole) and passive (eavesdropping, traffic monitoring, traffic analysis) are described.

Introduction

In Mobile Ad Hoc Networks (MANETs) has become one of the most prevalent areas of research in the recent years because of the challenges it pose to the related protocols. MANET is the new emerging technology which enables users to communicate without any physical infrastructure regardless of their geographical location, that's why it is sometimes referred to as an "infrastructure less" network. The proliferation of cheaper, small and more powerful devices make MANET a fastest growing network. An ad hoc network is self organizing and adaptive. Device in mobile ad hoc network should be able to detect the presence of other devices and perform necessary set up to facilitate communication and sharing of data and service. Ad hoc networking allows the devices to maintain connections to the network as well as easily adding and removing devices to and from the network. The set of applications for MANETs is diverse, ranging from large-scale, mobile, highly dynamic networks, to small, static networks that are constrained by power sources. Besides the legacy applications that move from traditional infrastructure environment into the ad hoc context, a great deal of new services can and will be generated for the new environment. It includes:

1. Military Battlefield

2. Sensor Networks

3. Medical Service

4. Personal Area Network.

Security solutions are important issues for MANET, especially for those selecting sensitive applications, have to meet the following design goals while addressing the above challenges. MANET is more vulnerable than wired network due to mobile nodes, threats from compromised nodes inside the network, limited physical security, dynamic topology, scalability and lack of centralized management. Because of these vulnerabilities, MANET are more prone to malicious attacks. The primary focus of this work is to provide a survey on various types of attacks the affect the MANET behavior due to any reason.

The dissertation first presents a scalable routing protocol that applies a hierarchical structure. Then, the dissertation presents three routing optimization techniques: salvaging route reply, multiple-target route discovery, and bilateral route discovery. Finally, the dissertation presents a generalized and efficient scheme to support high-throughput routing metrics

Conventional topology-based multicast protocols include tree-based protocols and mesh-based protocols .Tree-based protocols construct a tree structure for more efficient forwarding of packets to all the group members. Mesh-based protocols expand a multicast tree with additional paths which can be used to forward packets when some of the links break. Although efforts were made to develop more scalable topology-aware protocols, the topology-based multicast protocols are generally difficult to scale to a large network size, as the construction and maintenance of the conventional tree or mesh structure involve high control overhead over a dynamic network. The work in attempts to improve the stateless multicast protocol, which allows it a better scalability to group size. In contrast, EGMP uses a location-aware approach for more reliable membership management and packet transmissions, and supports scalability for both group size and network size. As the focus of our paper is to improve the scalability of location-based multicast, a comparison with topology-based protocols is out of the scope of this work. However, we note that at the similar mobility and system set-up, the delivery ratio of is much lower than that of EGMP, and the delivery ratio in varies significantly as the group size changes. In addition, topology-based routing by nature is more vulnerable to mobility and long path transmission, which prevents topology-based protocols from scaling to a large network size.

Modules:
1. Efficient Geographic Multicast Protocol
2. Multicast Tree Construction
3. Multicast group join
4. Packet sending from the source
5. Multicast data forwarding
6. Multicast Route Maintenance and Optimization

Module Description:

1. Efficient Geographic Multicast Protocol

EGMP supports scalable and reliable membership management and multicast forwarding through a two-tier virtual zone- based structure. At the lower layer, in reference to a pre-determined virtual origin, the nodes in the network self-organize themselves into a set of zones as shown in

Figure 1

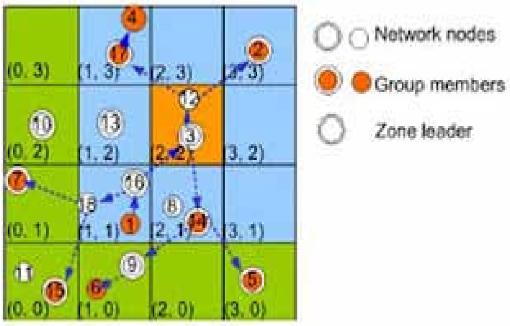
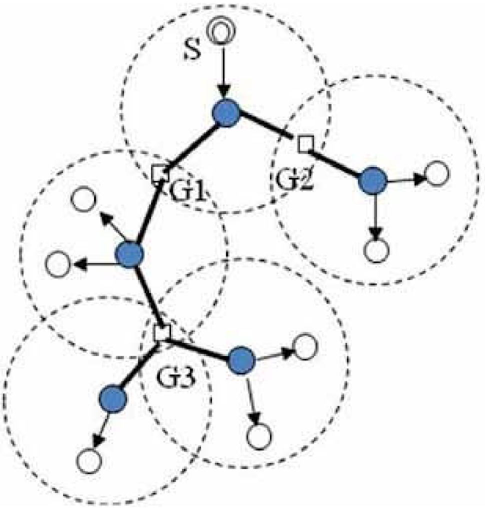


Fig. 1 and a leader are elected in a zone to manage the local group membership. At the upper layer, the leader serves as a representative for its zone to join or leave a multicast group as required. As a result, a network-wide zone-based multicast tree is built. For efficient and reliable management and transmissions, location information will be integrated with the design and used to guide the zone construction, group membership management, multicast tree construction and maintenance, and packet forwarding.

2. Construction of Multicast Tree

We present the multicast tree creation and maintenance schemes. In EGMP, instead of connecting each group member directly to the tree, the tree is formed in the granularity of zone with the guidance of location information, which significantly reduces the tree management overhead. With a destination location, a control message can be transmitted immediately without incurring a high overhead and delay to find the path first, which enables quick group joining and leaving.

3. Multicast group join

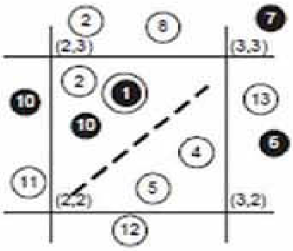


When a node M wants to join the multicast group G, if it is not a leader node, it sends a JOIN REQ(M; PosM; G; fMoldg) message to its zLdr, carrying its address, position, and group to join. The address of the old group leaderMold is an option used when there is a leader handoff and a new leader sends an updated JOIN REQ message to its upstream zone. If M did not receive the NEW SESSION message or it just joined the network.

4. Packet sending from the source

After the multicast tree is constructed, all the sources of the group could send packets to the tree and the packets will be forwarded along the tree. In most tree-based multicast protocols, a data source needs to send the packets initially to the root of the tree. If this scheme is used and node 5 in Fig. 1 is a source, node 5 needs to uni-cast the packets initially to root zone (2, 2). The sending of packets to the root would introduce extra delay especially when a source is far away from the root. Instead, EGMP assumes a bi-directional tree- based forwarding strategy, with which the multicast packets can flow not only from an upstream node/zone down to its downstream nodes/zones, but also from a downstream node/zone up to its upstream node/zone.

5. Multicast data forwarding



Maintain the multicast table, and the member zones normally cannot be reached within one hop from the source. When a node N has a multicast Packet to forward to a list of destinations (D1; D2; D3; :), it decides the next hop node towards each destination (for a zone, its center is used) using the geographic forwarding strategy. After deciding the next hop nodes, N inserts the list of next hop nodes and the destinations associated with each next hop node in the packet header. An example list is (N1: D1; D3; N2: D2; :), whereN1 is the next hop node for the destinations D1 and D3, and N2 is the next hop node for D2. Then N broadcasts the packet promiscuously (for reliability and efficiency). Upon receiving the packet, a neighbor node will keep the packet if it is one of the next hop nodes or destinations, and drop the packet otherwise. When the node is associated with some downstream destinations, it will continue forwarding packets similarly as done by node N.

6. Maintenance and Optimization of Multicast Route

In the zone structure, due to the movement of nodes between different zones, some zones may become empty. It is critical to handle the empty zone problem in a zone-based protocol. Compared to managing the connections of individual nodes, however, there is a much lower rate of zone membership change and hence a much lower overhead in maintaining the zone-based tree.

When a member node moves to a new zone, it must rejoin the multicast tree through the new leader. When a leader is moving away from its current zone, it must handover its multicast table to the new leader in the zone, so that all the downstream zones and nodes will remain connected to the multicast tree.

Objectives of the study:

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. 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.

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.

Conclusions

There is an increasing demand and a big challenge to design more scalable and reliable multicast protocol over a dynamic ad hoc network (MANET). In this paper, we propose an efficient and scalable geographic multicast protocol, EGMP for MANET.

The scalability of EGMP is achieved through a two-tier virtual-zone-based structure, which takes advantage of the geometric information to greatly simplify the zone management and packet forwarding. We make a quantitative analysis on the control overhead of the proposed EGMP protocol and our results indicate that the per-node cost of EGMP keeps relatively constant with respect to the network size and the group size. We also performed extensive simulations to evaluate the performance of EGMP.

Our results indicate that geometric information can be used to more efficiently construct and maintain multicast structure, and to achieve more scalable and reliable multicast transmissions in the presence of constant topology change of MANET. Our simulation results demonstrate that EGMP has high packet delivery ratio, and low control overhead and multicast group joining delay under all cases studied, and is scalable to both the group size and the network size. Compared to the geographic multicast protocol SPBM, it has significantly lower control overhead, data transmission overhead, and multicast group joining delay

REFERENCES

• X.Xiang, X.Wang, and Y. Yang, "Supporting Efficient and Scalable Multicasting over Mobile Ad Hoc Networks", IEEE Transactions on Mobile Computing, Vol. 10, No.4, April 2011. | • B. Fenner, M. Handley, H. Holbrook, and I. Kouvelas, "Protocol Independent Multicast – Sparse Mode (PIM-SM): Protocol Specification (Revised)," RFC 4601, IETF Network Working Group, 2006. | • GlobalSecurity.org (2007), "Unmanned Aerial Vehicles," Retrieved May 5, 2007 from http://www.globalsecurity.org/intell/systems/uav-intro.htm | • V. Hubenko, "Secure and efficient communications for global information grid users via cooperating space assets," PhD Prospectus, Dept. of Elect. and Comp. Eng., Air Force Institute of Technology, Wright-Patterson AFB, OH, 2006. | • M. T. Hyland, B. E. Mullins, R. O. Baldwin, and M. A. Temple, "Simulation-based Performance Evaluation of Mobile Ad Hoc Routing Protocols in a Swarm of Unmanned Aerial Vehicles," IEEE International Symposium on Pervasive Computing and Ad Hoc Communications (PCAC-07), Niagara Falls, Canada, May 2007. | • P. Judge and M. Ammar, "Security issues and solutions in multicast content distribution: a survey," IEEE Network, vol. 17, no. 1, pp. 30-36, 2003. | • United States Air Force, The U.S. Air Force Remotely Piloted Aircraft and Unmanned Aerial Vehicle Strategic Vision, 2005. Available: http://www.af.mil/shared/media/document/AFD-060322-009.pdf.