Comparative Analysis Of Multicasting Routing Protocols With Security Model In MANETs

Shruti Sharma Manisha Sharma

Abstract

Mobile Ad-hoc networks have been the focus of research interest in wireless networks. An ad-hoc network is a collection of wireless mobile nodes dynamically forming a temporary network without the use any existing network infrastructure or centralized administration. Mobile ad-hoc networks are open to a wide range of attacks due to their unique characteristics like open medium, dynamically changing topology, absence of infrastructure, resource constraint and trust among nodes. This paper focuses on the comparison between two Multicast Routing Protocols AAMRP and Improved ODMR (IODMRP) with SB-PGP security Model.

1. INTRODUCTION

MANET is a multi-hop wireless network with no fixed infrastructure or central administration. Due to their inherent broadcast capability, ad hoc networks are well suited for multicast. To support multicast, an efficient multicast routing protocol is required for ad hoc networks because of their characteristics. Also, nodes in MANETs are totally independent from any centralized device and they are free to move anywhere. This causes suddenly appearance and disappearance of the nodes and moving of nodes from one place to another place also increases the probability to compromise. Another issue in mobile ad hoc networks is that the nodes are resource constraint. Nodes are totally dependent on battery power and have limited memory and bandwidth. Therefore, security requirements such as authentication, integrity, availability, confidentiality, and nonreputation should be guaranteed during the communication between source and destination. Mobile nodes communicate via wireless links if they are in transmission range of each other. Each node behaves as a router in order to forward data packets. Routers moves in randomly free manner.

2. Routing in MANETs

Routing in MANETs is to find and maintain routes between nodes in a dynamic topology with possibly using minimum resources. Routing in MANETs is a dynamic optimization task aiming at providing paths that are:

• Optimum in terms of some criterion (e.g. minimum distance, maximum bandwidth, shortest delay).

• satisfying some constraints (e.g. limited power of mobile nodes, limited capacity of wireless links).

The routing concept basically involves, two activities: firstly, determining optimal routing paths and secondly, transferring the information groups (called packets) through an internetwork.

3. Routing Protocols

An ad-hoc routing protocol is a set of rules, or standard, that controls how nodes decide which way to route packets between computing devices in a mobile ad hoc network. In ad-hoc networks, nodes are not familiar with the topology of their networks. Instead, they have to discover it. The basic idea is that a new node may announce its presence and should listen for announcements broadcast by its neighbors. The main objectives of MANET routing protocols are to maximize network throughput, to maximize network lifetime, to maximize energy efficiency and to minimize delays. The network throughput is measured by packet delivery ratio and energy contribution is measured by routing overhead which is number or size of routing control packets.

4. Need of Routing Protocols

- Nodes in ad hoc networks are mobile and the topology of interconnections between them may be quite dynamic.
- Existing protocols exhibit least desirable behavior when presented with a highly dynamic interconnection topology.
- Existing routing protocols place a too heavy computational burden on each mobile computer in terms of the memory-size, processing power and power consumption.

- Existing routing protocols are not designed for dynamic and self-starting behavior as required by users wishing to utilize ad hoc networks.
- Existing routing protocols like the Distance Vector Protocol take a lot of time for convergence upon the failure of a link, which is very frequent in ad hoc networks.
- Existing routing protocols suffer from looping problems either short lived or long lived.
- Methods adopted to solve looping problems in traditional routing protocols may not be applicable to ad hoc networks.

5. Multicast Routing

Multicasting can be defined as transmission of data packets to several destinations at the same time. Transmitter may be a single or multiple nodes which are said to be "one to many" nodes or "many to many" nodes.

In general multicast routing is achieved using either

• Source based-when no. of multicast senders in a group is small (e.g.-video on demand application)

• Core based trees-uses a multicast tree shared by all members of a group.

Multicast forwarding is based on nodes rather than on links.

6. Multicast Routing Protocols

6.1 Improved On-Demand Multicast Routing Protocol (IODMRP)

IODMRP is the enhanced result of ODMRP. It is a more efficient multicast routing protocol. It chooses partial forwarding nodes to relay packets, the number of which is decided by probabilistic forwarding algorithm based on forwarder's density and the nodes are selected according to energy state. This protocol is implemented through simple modifications to existing ODMRP, But the redundant data transmission is reduced and save energy significantly through decreasing the forwarding packets. It employs the algorithm of self-adapting probability, which means adjusting probability according to local density of forwarders. When the number of neighbor forwarding nodes is small the probability is 100% to guarantee high packet delivery ratio, on the contrary play down the probability to cut down partial contention and congestion, hence the transmission efficiency is heightened and the performance of the network is improved. The establishing and updating of the forward structure in IODMRP is the same as ODMRP. It has a better end to end delay and delivery ratio.

6.2 Ant Based Adaptive Multicast Routing Protocol (AAMRP)

AAMRP dynamically identifies and organizes the group members into clusters which correspond to areas of high group member affinity. In each of these "dense" neighborhoods, one of the group members is selected to be a cluster leader. Cluster leaders have two main functions:

- They establish a sparse multicast structure among themselves and the source, and
- They use broadcasting (with adaptive scope) to deliver the packets to other group members in their cluster.

It constructs a 2-tier hierarchical structure, where the upper tier is formed by a multicast source and cluster leaders that represent groups of multicast members that form a cluster, and the lower tier consists of the members in a cluster. Each cluster demonstrates a high density of group members; a cluster leader simply invokes an adaptive localized broadcast within its cluster to disseminate multicast packets received from the source. Each group member in AAMRP can be in 3 states. It can be in a temporary mode wherein it is JOINING the session, it can be cluster LEADER, or it can simply be the MEMBER of a cluster leader. Each node maintains a Group Member Table (GMTable) which contains the information of the joining group members. The information maintained in this table is obtained by means of the ADVERTISE and the LEADER messages. Each cluster leader maintains a Cluster Member Table (CMTable), which contains information of all the cluster group members that are associated with the cluster leader. The information maintained in the table is obtained via the reception of MEMBER messages that are sent out by each cluster member.

7. SB-PGP (Seniority Based Pretty Good Privacy) Model

7.1 PGP-Based Solutions

The 'Public Key Infrastructure' (PKI) is the most scalable form of key management. Several different PKI techniques exist, such as SPKI, PGP and X.509. In group-oriented PKI, The leader of the group acts as a 'Certificate Authority' (*CA*), which issues group membership certificates. These are said to be SPKI-style certificates. They certify that the public key in the certificate belongs to a group member. PGP allows users to create, store, distribute, and revoke their public keys without the help of any trusted authority or fixed server. In PGP, any node can issue a certificate and as such it allows a completely distributed architecture, apart from the central repository, which holds these certificates. This scheme involves each node keeping mini-repositories, which hold all the certificates the node issues and all the certificates issued on it. When nodes *A* and *B* meet, they merge their mini repositories. The repositories are constructed according to the 'Shortcut Hunter algorithm". This algorithm constructs repositories such that two nodes merging repositories have a high probability of finding a chain of certificates between them if one exists. This scheme is useful in a civilian environment where delegation of trust through a number of nodes is acceptable. Let the notation *A* → *B* mean that *A* trusts *B*. Then what the implications *A* → *B*, *B* → *C*, *C* → *D* and *D* → *E* signify is that *A* chooses to trust *E* i.e. *A* → *E*. An alternative approach is to use a Certificate Authority (*CA*) to issue certificates. A *CA* is a third party trusted by all in the system, which effectively eliminates the need for a repository of certificates. Rather than finding a certificate linking *A* → *B* → *C* → *D* → *E*, one simply recovers the certificate *A* → *E*. As such, the *CA* can be seen as a one-hop shortcut through the web of trust. The problem with this is the *CA* must be trusted by all and becomes a single point of failure in the event of an attack.

7.2 The SB-Trust Model

In PGP's "web-of-trust" model , each entity manages its own trust based on direct recommendation and seeks to further quantify the notions of trust and recommendation it uses a seniority-based (SB) trust model which is as follows. Trust management and maintenance are distributed in both space (*k*) and time (*T*) domains in the SB-model. Thus SB-model describes a seniors-securing approach to node authentication in MANET. In other words, the parameter *T* characterizes the time varying feature of a trust relationship, while *k* signifies the number of senior nodes required to work as *CA*. An entity is trusted if any *k* trusted available senior entities claim so within a certain time period *T*. Once a node is trusted by its senior group, it is globally accepted as a trusted node. Otherwise, if the seniors distrusted an entity then it is regarded as untrustworthy in the entire network. If a node cannot find *k* senior nodes in certain network, it may roam to meet more nodes or wait for new senior nodes to move in.

8. Related Work

SBPGP is giving better security as compared to the other techniques of PKI model. A study is performed for comparison analysis for SBPGP model with PGP security models. It showed that SBPGP gives better results and gives better security [2]. The comparison between ODMRP and IODMRP protocols is carried out based on the three metrics to see which protocol is better among these two multicast protocols. From the results, it can be said that IODMRP is performing in a better manner than ODMRP. In future these protocols can also be implemented with other security models like pretty good privacy etc and can be comparison can be done between other protocols also [4]. Ant agent based adaptive multicast protocol combines the positive aspects both multicasting and broadcasting .It exploits group members' desire to simplify multicast routing and invoke broadcast operations in appropriate localized regimes. By reducing the number of group members that participate in the construction of the multicast structure and by providing robustness to mobility by performing broadcasts in densely clustered local regions, the proposed protocol achieves packet delivery statistics that are comparable to that with a pure multicast protocol but with significantly lower overheads. By the simulation results, it has been showed that proposed protocol achieves increased PDF with reduced overhead and routing load [3].

9. Proposed Methodology

- Creation a Wireless Network.
- Installation of Network Simulator Version 2.
- Implementation of IODMR Protocol in NS2. Implementation of AAMR Protocol in NS2. Implementation of Seniority Based Pretty Good Privacy Model in NS2.
- Integrate the Security Model with IODMRP and AAMR
- Compare the performance of security model with performance of IODMRP and AAMRP

10. Conclusion and Future Scope

In this paper we have studied two multicast routing protocols i.e. IODMRP and AAMRP. SB-PGP security model can be used effectively in such situations. In future these two protocols can be compared individually and then with the performance of SB-PGP security model. Then the results can be used to analyze the performance and further research in this field.

References

[1] Ying-xin Hu, Yu-feng Jia, "Improvement of Wireless Multicast Routing with Energy-efficiency based on ODMRP" IEEE 2009.

[2] Jashanvir Kaur, Er. Sukhwinder Singh Sran," SBPGP Security based Model in Large Scale Manets" published in International Journal of Wireless Networks and Communications. ISSN 0975-6507 Volume 4, Number 1 (2012), pp. 1-10.

[3] A. Sabari, K.Duraiswamy, “Ant Based Adaptive Multicast Routing Protocol (AAMRP) for Mobile Ad Hoc Networks” published in (IJCSIS) International Journal of Computer Science and Information Security, Vol.6, No. 2, 2009.

[4] Shavinder, Sandeep Kang, “Comparative Analysis of ODM and IODM Routing Protocols with PKC Security Model in MANETS” published in IJECT Vol. 2, Issue 3, Sept. 2011.

[5] E. A .Mary Anita, V. Vasudevan, “Black Hole Attack Prevention in Multicast Routing Protocols for Mobile Ad hoc networks using Certificate Chaining” published in International Journal of Computer Applications (0975 – 8887) Volume 1 – No. 12, 2010.

[6] R. Manoharan, E. Ilavarasan, “Impact of Mobility on the performance of Multicast routing protocols in MANET” published in International Journal of Wireless & Mobile Networks (IJWMN), Vol.2, No.2, May 2010.

[7] Eslam Al Maghayreh, Salam Abu Al-Haija, Faisal Alkhateeb, Shadi Aljawarneh, “Bees Ants Based Routing Algorithm” published in International Conference on Intelligent Systems, Modelling and Simulation, 2010.

[8] Makoto Ikeda, Masahiro Hiyama, Leonard Barolli, Fatos Xhafa, Arjan Durresi, “Mobility Effects on the Performance of Mobile Ad hoc Networks” published in International Conference on Complex, Intelligent and Software Intensive Systems, 2010.

[9] G.Varaprasad, P.Venkataram, “The Analysis of Secure Routing in Mobile Adhoc Network” in International Conference on Computational Intelligence and Multimedia Applications 2007.

[10] Kamal Kumar Chauhan, Amit Kumar Singh Sanger, Virendra Singh Kushwah, “Securing On-Demand Source Routing in MANETs” in Second International Conference on Computer and Network Technology.

[11] Q. Niu, “Secure On-Demand Source Routing for Ad hoc Networks”, Proceeding of IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 08), October, 2008, pp: 1-4. 297.

[12] Maqsood Razi, Jawaid Quamar, “ A Hybrid Cryptography Model for Managing Security in Dynamic Topology of MANET” published in IEEE 2008.