Secured wireless multicast group management protocol

Rajesh Perumal R.[1], Dr. P. Vanaja Ranjan[2]
[1]*Department of Embedded System Technologies, College of Engineering Guindy*
[2]*Professor, Department of Embedded System Technologies, College of Engineering Guindy*

***Abstract*— IGMP(Internet Group Management Protocol) is an integral part of IP multicast in wired networks. When it is used over wireless links, the amount of overhead increases significantly due to joint operation and the polling of mobile users by routers. And IGMP Joint is also having security threats such as local subnet attacks, subnet attack. Therefore it is inefficient and unsecured to implement IGMP Joint directly into wireless domain. The new method that we adopt should consider few facts, they are: Already the network is flooded with enough rate of control packets; Solution should maintain the multicast model as much as possible; Solution should minimize the introduction of using new functions. The proposed Secured Wireless Group Management Protocol(S-WMGMP) acts based on a alive-time-interval mechanism for join operation, considering the number of subscribers are sparse in the domain. Basic working prototype has been simulated and the results are good enough to go.**

***Index Terms*—Wireless Multicast, Alive-time-interval, Goup Management, Sparse mode.**

I. INTRODUCTION

IP multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to potentially thousands of corporate recipients and homes. Applications that take advantage of multicast include video conferencing, corporate communications, distance learning, and distribution of software, stock quotes, and news.

IP multicast delivers application source traffic to multiple receivers without burdening the source or the receivers while using a minimum of network bandwidth. Multicast packets are replicated in the network at the point where paths diverge by routers enabled with Protocol Independent Multicast (PIM) and other supporting multicast protocols, resulting in the most efficient delivery of data to multiple receivers.

Many alternatives to IP multicast require the source to send more than one copy of the data. Some, such as application-level multicast, require the source to send an individual copy to each receiver. Even low-bandwidth applications can benefit from using IP multicast when there are thousands of receivers. High-bandwidth applications, such as MPEG video, may require a large portion of the available network bandwidth for a single stream. In these applications, IP multicast is the only way to send to more than one receiver simultaneously

Multicast is based on the concept of a group. A multicast group is an arbitrary group of receivers that expresses an interest in receiving a particular data stream. This group has no physical or geographical boundaries—the hosts can be located anywhere on the Internet or any private internetwork. Hosts that are interested in receiving data flowing to a particular group must join the group using IGMP(Internet Group Management Protocol).

On the group management model of multicast, a sender only has to send a packet to a group address and the routers conspire to forward the packets to all the members of the group. This means, however, that a receiver may become a member of a group simply by listening on the multicast address for the group and no consent of the sender is needed. To achieve privacy and security on the broadcast model of multicast, transmissions must be encrypted and receivers may sometimes need to be authenticated at a protocol layer higher than the network.

The proposed Secured Wireless Group Management Protocol(S-WGMP) acts based on a increasing-interval mechanism, considering the number of subscribers are sparse in the domain, which limits the flooding of control packets among the mobile nodes. This approach minimizes the overhead of polling of mobile nodes and the communication is protected over wireless domain using an encryption

scheme (which can be configured by the user). And the encryption scheme should always perform well to keep up with the Line-rate traffic (at least 75%) of the Routers.

And an application with the help of this Wired-Multicast Protocol is checked in the project work. Solar power panels monitoring through the multicast service can be done with less energy consumption.

II. SCOPE

A. *Objectives*

- To develop a multicast group management group joining algorithm which will be more efficient than IGMP in Wireless domain, providing less overhead of control packets.
- To develop a multicast group management algorithm which will be more secured in Wireless domain, providing less overhead of cryptic process (Maintaining atleast 75% Line rate traffic).
- To develop multicast group Joining management algorithm ,this will not increase the flooding of control packets

B. *Challenges*

- Study and analysis of Group Management Protocol's Crypt Analysis to adopt a method of Security.
- Network analysis of any fault in the Algorithm.
- Programming the Joint Algorithm without bugs.

III. IP MULTICAST AND IGMP VERSIONS

1. *IP multicast*

IP multicast provides a scheme, allowing a host to send packets to a subset of all hosts (group transmission). Hosts must be a member of the group to receive the data stream. IP multicast addresses specify a "set" of IP hosts that have joined a group and are interested in receiving multicast traffic designated for that particular group. IPv4 multicast address conventions are described below.

The Internet Assigned Numbers Authority (IANA) controls the assignment of IP multicast addresses. IANA has assigned the IPv4 Class D address space to be used for IP multicast. Therefore, all IP multicast group addresses fall in the range from 224.0.0.0 through 239.255.255.255. The Class D address range is used only for the group address or destination address of IP multicast traffic. The source address for multicast datagrams is always the unicast source address.

Addresses in the range from 224.0.1.0 through 238.255.255.255 are called globally scoped addresses. These addresses are used to multicast data between organizations and across the Internet. Some of these addresses have been reserved for use by multicast applications through IANA. For example, IP address 224.0.1.1 has been reserved for Network Time Protocol (NTP). IP addresses reserved for IP multicast are defined in RFC 1112, Host Extensions for IP Multicasting.

Hosts join multicast groups by sending IGMP report messages. Many multimedia applications involve multiple participants. IP multicast is naturally suitable for this communication paradigm. IGMP is the traditional Group Management protocol used in wired networks.

2. *IGMP versions*

IGMP is used to dynamically register individual hosts in a multicast group on a particular LAN. Hosts identify group memberships by sending IGMP messages to their local multicast router. Under IGMP, routers listen to IGMP messages and periodically send out queries to discover which groups are active or inactive on a particular subnet.

In Version 1, only the following two types of IGMP messages exist: Membership query, Membership report.

Hosts send out IGMP membership reports corresponding to a particular multicast group to indicate that they are interested in joining that group. The TCP/IP stack running on a host automatically sends the IGMP Membership report when an application opens a multicast socket. The router periodically sends out an IGMP membership query to verify that at least one host on the subnet is still interested in receiving traffic directed to that group. When there is no reply to three consecutive IGMP membership queries, the router times out the group and stops forwarding traffic directed toward that group.

In Version 2, the following four types of IGMP messages exist: Membership query, Version 1 membership report, Version 2 membership report,

Leave group. IGMP Version 2 works basically the same way as Version 1. The main difference is that there is a leave group message. With this message, the hosts can actively communicate to the local multicast router that they intend to leave the group. The router then sends out a group-specific query and determines if any remaining hosts are interested in receiving the traffic. If there are no replies, the router times out the group and stops forwarding the traffic. The addition of the leave group message in IGMP Version 2 greatly reduces the leave latency compared to IGMP Version 1. Unwanted and unnecessary traffic can be stopped much sooner.

In IGMPv3, the following types of IGMP messages exist: Version 3 membership query, Version 3 membership report. IGMPv3 supports applications that explicitly signal sources from which they want to receive traffic. With IGMPv3, receivers signal membership to a multicast host group in the following two modes:

•INCLUDE mode—In this mode, the receiver announces membership to a host group and provides a list of source addresses (the INCLUDE list) from which it wants to receive traffic.

•EXCLUDE mode—In this mode, the receiver announces membership to a multicast group and provides a list of source addresses (the EXCLUDE list) from which it does not want to receive traffic. The host will receive traffic only from sources whose IP addresses are not listed in the EXCLUDE list. To receive traffic from all sources, which is the behavior of IGMPv2, a host uses EXCLUDE mode membership with an empty EXCLUDE list.

IV. ISSUES IN IGMP OVER WIRELESS

Overhead

When the IGMP is used over wireless links, the amount of overhead increases significantly due to joint operation and the polling of mobile users by routers.

Expectations from proposed approach

The new method that we adopt should consider few facts, they are:

- Already the network is flooded with enough rate of control packets
- Encryption should be simple as it should not consume much power

V. PROPOSED ALGORITHM

A. Considerations

Because of the uncertainty of the wireless medium, there are few considerations to employ this algorithm.

- The Network must be an infrastructure based wireless network
- All the Join messages will be sent to 224.0.0.1 IP address and the Leave messages will be sent to 224.0.0.2 IP address.

B. Algorithm to Join and Leave a group from host

1) Receiver Host sends a Join message to the host indicating that it wants to subscribe to the service using a (*,G) Join, where '*' stands for the source address of the origination of multicast data and G stands for the Group Address

2) When the Host want to stop the subscription of the channel, Receiver Host sends a Leave message to the host indicating that it wants to unsubscribe to the service using a (*,G) Leave, where '*' stands for the source address of the origination of multicast data and G stands for the Group Address

3) When the Host goes down by any means (low battery, shut-down and restart), it will send a Leave message and sends a Join when the host comes up again.

4) Whenever the host sends a Join, it will include "Alive-Time-interval" in the message to specify ,until when the connection to be retained, without control packet exchange.

5) If the host doesn't receive any data for more than half of Alive-Time-interval, the host will retrigger a Join message.

C. Security for WMGMP to make it S-WMGMP

The most sensitive part of the multicast messages are Alive-Time-interval and Group address to be joined. These two are to be encrypted using an encryption scheme which is pre-informed by one of the standard security models such as IPsec.

In this paper we use an encryption algorithm, which is based on Kolam pattern. This algorithm is based on binary transportation and permutation, which consumes very less amount of power on wireless nodes.

D. Encryption sample code

/*Encrypt part, "a" is array which contains the plaintext*/

while(k<25)

```
{    cipher_binary[i][j] = a[KeyRow[k]][KeyCol[k]];
    j++;
   if(j == 5)
   {
     if(i<=3)
    {       i++;     }
     else      if(i == 4)
    {         break;     }
     j=0;
   }
   k++;
}

/*Decrypt part, "cipher_binary" is array which contains the chipertext*/
for(k=0;k<25;k++)
{
   plain_binary[(PVRKey[k]/10)                    -1][(PVRKey[k]%10) -1] = cipher_binary[i][j++];
   if(j == 5)
   {
      if(i<=3)
      { i++;  }
      else if(i == 4)
      {  break;  }
            j=0;
       }
 }
```

MIB design for S-WMGMP

S-WMGMP can use the MIB of IGMP with an addition to have a table for maintaining members of the Groups and Alive-time-interval, which should be designed in future research work. As per the MIB data-structures it should have the name and as shown below,

```
WmgmpMemberAliveTime OBJECT-TYPE
                SYNTAX     Gauge32
                MAX-ACCESS read-write
                STATUS     current
                DESCRIPTION                "Alive
```

time in seconds since the last WMGMP Join message was received from the member. Each time WmgmpMemberAliveTime is set with value from the Join message . The value of this object is set to zero (0). "

Other than the above mentioned new MIB, the existing IGMP standard MIB should also be used for maintaining the interface status information and Group Cache information.

VI. EXPERIMENTATION RESULTS

A. Performance testing of encryption scheme

Encryption Scheme has been applied to Various Network processors to check the Performance in the live wired network. And it returned a good performance

TABLE I: ENCRYPTION SCHEME TESTING

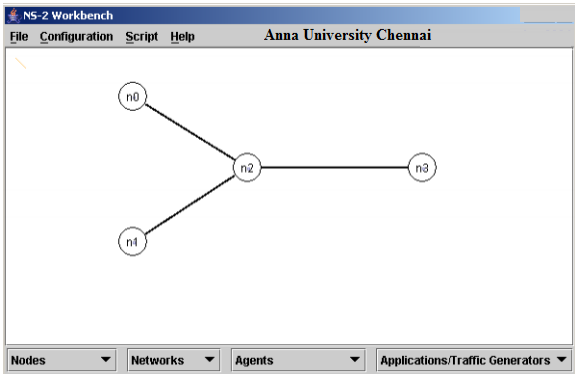
Target Chipset	**Performance testing**		
	Rate of traffic sent	***Rate of traffic received***	***Performance***
Broadcom (56440)	1Gb/s	748Mb/s	75%
Broadcom (56850)	10Gb/s	7.9Gb/s	79%

B. Simulation of multicast Joint model

The S-WMGMP has been simulated with the help of NS2(Network Simulator). Four nodes were used, two of them acted as hosts(which receives service). One node is acted as a source for multicast delivery .Steps used,

- Node-0 and Node-1 send Join Messages to neighbor router for getting service from 232.0.0.1 and 232.0.0.2 respectively.
- As soon as the neighbor forwards the request to the source(Node-3), it starts transmitting to Node-0 and Node-1 via the neighbor router.
- The Node-0 and Node-1 has been restarted multiple times and it has been checked, if the algorithm works fine.
- In the meanwhile, one more node(Node-4) added and sent DDoS Subnet attack packets to gain access to modify the host information in Neighbor router.

Fig 1 : NS2: Multicast toplogy



Moteview: IRIS-motes topology

All the mentioned steps had been done for S-WMGMP and IGMP.

Comparison results with IGMP

The IGMP and S-WMGMP are compared through few parameters such as efficiency, security, power consumption and host-reboot scenario.

COMPARISON: IGMP VS S-WMGMP

Test description	**Comparison**		
	IGMP	***S-WMGMP***	***Observation of S-WMGMP***
Subnet attack	Topology unsettled and delay in packets	There is no disturbance to topology	Masks subnet attack
Restart and ShutDown	Topology resettled after a delay of 2second	Topology resettled after a delay of 0.5 second	~75% more efficient in timeliness

S-WMGMP proves to be better in Node Reboot test and security tests.

VII. CONCLUSION

In this paper, Secured Wireless Multicast Group Management Protocol for Group management joint function has been designed, the encryption algorithm for security has been tested, the four node topology to simulate the application of the multicast model has been implemented and tested in NS2. From the design perspective of S-WMGMP and from the wide usage of IGMP, it is feasible to implement the S-WMGMP in wireless networks. Future research work to be done on realizing the multicast model on live network environment and practicality to be studied.

ACKNOWLEDGMENT

The authors gratefully acknowledge Department of Embedded System Technologies of Anna University Chennai(College of Engineering Guindy) for providing Lab and Equipments support to carry out this research work.

REFERENCES

[1]. http://en.wikipedia.org/wiki/IP_multicast

[2]http://www.cisco.com/c/en/us/td/docs/ios/solutions_docs/ip_multicast/White_papers/mcst_ovr.html

[3] H. Asaeda, et al "Tuning the Behavior of the Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) for Routers in Mobile and Wireless Networks" IETF 2012

[4] Brian Coan, et al "IGMP Security Problem Statement and Requirements" IETF GSEC 2002

[5] Upkar Varshney, "Multicast Over Wireless Networks" COMMUNICATIONS OF THE ACM December 2002/Vol. 45, No. 12

[6] Lu Su, et al "oCast: Optimal Multicast Routing Protocol for Wireless Sensor Networks" CNS-0916171 2010

[7] R.Periasamy, et al "A Study on Multicast Routing Protocols for MANETS: MRMP, ERAMOBILE, TSMP, LAM, PUMA" IJCSNS 2013

[8] W. Fenner, et al "Internet Group Management Protocol, Version 2" IETF 2006

[9] B. Fenner, et al "Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (Revised) " IETF 2006

[10] B. Cain, et al "Internet Group Management Protocol, Version 3" IETF 2002

[11] H. Liu, et al "IGMP/MLD Optimizations in Wireless and Mobile Networks draft-ietf-pim-igmp-mld-wireless-mobile-" IETF 2014

[12] A. Van Moffaert, et al "Security issues in Internet Group Management Protocol version 3 (IGMPv3)" IETF 2002

[13] Wen Tau Zhu "Crypt Analysis For Two Group Key Management Protocols for secured multicast " Springer 2005
[14] Cisco Public "IP Multicast – Concepts, Design and Troubleshooting" CISCO 2011
[15] Katia Obraczka, et al "Multicast Routing Issues in Ad Hoc Networks" Hughes Research Laboratories (GP3044-97261) 2003
[16] Chris Conger, et al "Traffic Analysis Prevention" CIS6935 2003
[17] McCloghrie, et al "Internet Group Management Protocol MIB" IETF 2000