International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 31721-31726

http://www.ripublication.com

A Secure Robust On-Demand Multicast Routing Protocol Over Mobile Ad Hoc Networks

Seetha.R, R. Saravanan

School of Information Technology & Engineering, VIT University, Vellore
rseetha@vit.ac.in

ABSTRACT

Group communication involves one - many or many - many people communicating over their desired network. The importance of people communicating in groups over dynamic topology environment has led to the evolution of many multicast protocols. This paper presents a robust, scalable and a group authentication protocol for efficient and secure communication among the group members over the dynamic ad-hoc environment.

KEY TERMS: Scalability, Robust, Multicast, Authentication, Key agreement.

1.INTRODUCTION

The upcoming technology and popularity of Internet makes applications, such as video conferencing, which need multicast support, are becoming more common. Another interesting emergence is dynamically reconfigurable wireless ad hoc networks [1, 2] to interconnect mobile users. Ad hoc networks have no fixed infrastructure or central administration, and each node must communicate the other node via some packet transmission. Some of the applications of ad hoc networks include disaster recovery, crowd control, search and rescue, and automated battlefields. Nodes in ad hoc networks move randomly, making the network topology dynamic and unpredictable with limited resources of bandwidth and battery power.

Group communication can be implemented over application layer or network layer. Multicast at network layer level has more challenging tasks on comparing to application layer level.Themajor routing challenge is described below in Figure 1.1

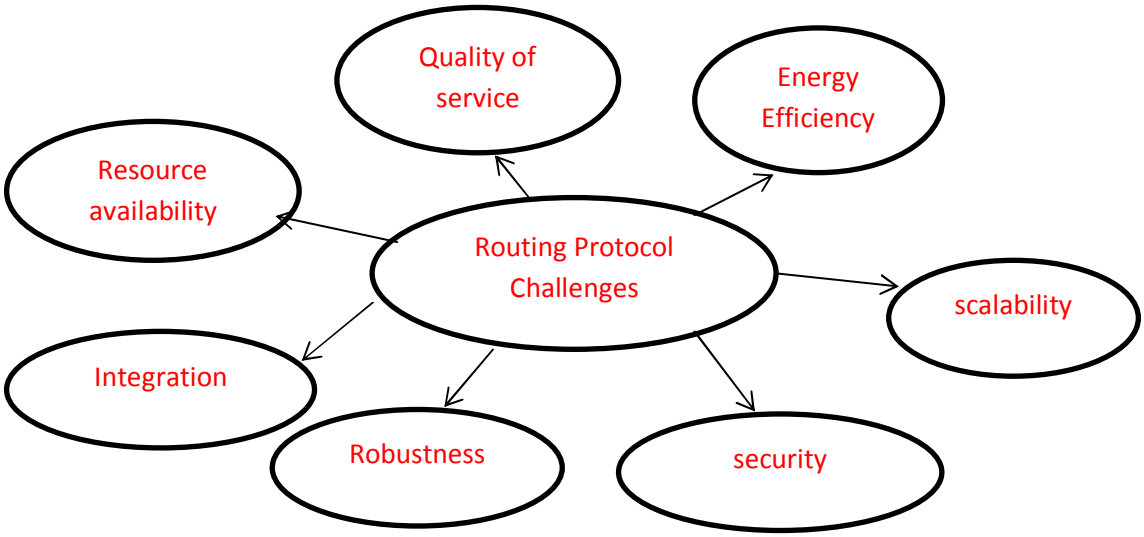

Figure 1.1 Major Routing Challenges

- Robustness: The ability of the protocol to provide an efficient communication among the nodes even when nodes move rapidly or there is frequent change in the topology.
- Scalability: A multicast routing protocol should allow any number of nodes to participate in the multicast session taking into consideration of ad hoc network characteristics such as resource constraints, mobile nodes and dynamic topological environment.
- Energy Efficiency: The use of power resources available efficiently by minimizing the overheads (storage, use of control packets) for successful multicast session.
- Integration: Adaptation of protocol to any environment.
- Resource Availability: The protocol must effectively use the limited available resources over the network it operates
- Security: The protocol should be capable of withstanding and attacks happening in the network environment.
- Quality of Service: QoS requirements include bandwidth availability, delay, delay jitter, and packet loss.

The paper mainly focuses on scalability issue and maintaining the stability of link established among the members of participating group.The basic security of the multicast session relies on the authentication mechanism and group key agreement scheme employed. The nodes joining the session are authenticated and rekeying process is carried out to preserve forward and backward secrecy.Authentication is the initial key part of the multicast session in order to allow only the legitimate members to get access to the session. The key agreement scheme is the second key part of the

multicast session as the success of the session relies on the secure transmission of group key over the unsecure dynamic ad hoc environment.

2. RELATED WORK

The authors of [7] has made a detailed study on tree based and mesh based multicast routing protocols and narrated advantages and disadvantages of such protocols. The details of key exchange mechanism are discussed in [6].

DineiFlorˆencio and Cormac Herley [4] describesa service that allows users to make use of one-time password (OTP). The authors also briefed on possible attacks on OTP and remedial measures to be taken against such attacks.Hani Alzaid[3], pinpoints in detail the importance of preserving forward and backward secrecy for secure group communication.LeinHarn and Changlu Lin [5]proposed an authenticated key transfer protocol based on secret sharing scheme and given a detailed analysis of security threats over the proposed protocol.

3. PROPOSED MULTICAST ROUTING PROTOCOL

The multicast protocol proposed is on demand based on the number of participating nodes. The multicast protocol is source initiated, scalable and robust in order to ensure reliability. Depending on the number of participating nodes (say ≤ 20) the nodes form tree based architecture with initiator node as the root. If the number of participating node increases (say > 20) the multicast communication reforms into core assisted mesh based architecture.

- Multicast session initiation: The node that initiates the session becomes the source node. The source node floods the JOINREQ packet containing source_id, session_idand list of forwading nodes over the network. The node who wants to join the session replies back with JOINREPLY packet along a shortest path of forwarding nodes. The forwarding nodes are trusted static nodes of the session.
- Authentication: The JOINREPLY packet from each participating node contains a nonce N and host name. The source node replies with a packet containing nonce N, host_id, One Time Password (OTP) and encrypts the packet using a one way hash function (SHA-1). The receiver applies the same hash function and retrieves back the details contained in the packet and checks whether its nonce N sent is the same. The node now joins the session using the host_id as username and OTP.

The OTP generated is a one-time password and can be used only once. If the node leaves and re-joins the group the node is re-authenticated with a new OTP that is generated randomly. The randomly generated OTP does not allow a node who joined recently to know what has happened in the past and the leaving node to know about what communication is transmitted in the future. Thus the protocol assures backward and forward secrecy.

- Multicast Topology: Based on the number of members participating, the multicast session either form a source based tree or a core based mesh topology. The structure of the session is decided based on a threshold value (th=20). If the number of participating nodes n>th then the session forms a core-based mesh topology. If the number of participating nodes n ≤ th then the session forms a source based tree topology.
- Group Key Agreement: Once the multicast group is set up the group key which plays a vital role for secure communication is exchange using the following algorithm technique.

Key Exchange Algorithm for secure group communication:
Let two nodes say, A and B are communicating.

- Either A or B chooses a large distinct prime numbers, say p and q.
- Compute M= p*q, Φ (n) = (p-1)*(q-1) and is made public.
- Now A chooses it's private key and generates a output pattern of private key using Linear Feedback Shift Registers (LFSR) [11, 13]. Using the key pattern (say X) of LFSR, A computes α= (M ⊕ X) mod Φ (n) (where ⊕ denotes XOR operation).
- Similarly B computes β = (M ⊕Y) mod Φ (n). (Where Y is the output key pattern of LFSR generated from private key of B).
- Both A and B exchanges α and β.
- Now A computes (β ⊕X) mod Φ (n) and B computes (α⊕ Y) mod Φ (n).

Both A and B has calculated public key which can be used to encrypt or decrypt the messages that they want to share.

The algorithm can be extended to multicast communication involving n (n>=3) parties. The key exchange algorithm uses the existing technique of multicast communication like liDivide and Conquer technique. The use of divide and conquer technique results in reducing the number of exchanges made among the participating nodes [12]. Consider four nodes say, A, B, C and D is participating in the communication.

- Node A computes α and sends to Node B.
- Node B computes BKEY= (α⊕ Y) mod Φ (n) sends to Node C and Node D.
- Node C computes γ and send to Node D.
- Node D computes DKEY= (γ⊕ W) mod n where W is the private key of D and sends to Node A and Node B.
- Node A computes (DKEY⊕ X) mod Φ (n) and sends to Node B.
- Node B computes (DKEY⊕ Y) mod Φ (n) and sends to Node A.
- Node A and B computes the final key using the LFSR generated private key and modulus operation.
- Similarly Node C and D compute the final key.

As the number of participating node increases the number of exchange made decreases drastically in divide and conquer technique and thus improves the

efficiency of time. The Table 1 figures out the time complexity of key exchanges made using divide and conquer technique among the various number of participating nodes in the multicast session.

Table 1: Time complexity of key exchanges made using Divide and conquer technique

No. of participating nodes	Divide and conquer technique
3	6
4	10
8	20
N	2n+n/2
	Time Complexity= $O(\log_2 n)+1$

4. RESULTS AND DISCUSSION

The proposed multicast protocol mainly focuses on robustness, multicast efficiency and control overhead. The degree of robustness and the packet delivery ratio are directly proportional but inversely proportional to control overhead. The proposed on demand protocol is capable of handling both small members of group as well as large members of the group.Making the multicast structure to be on demand, scalability is extended and thus increasing the degree of robustness by forming a core based mesh structure when the number of participating node increases (say n>th=20).

The use of OTP provides a solution for major secrecy issues of group communication like forward secrecy and backward secrecy when a participating node leaves the group or a member newly joins or re-joins the group.

The key exchange mechanism employed for secure multicast session also improves the multicast efficiency. The use of divide and conquer technique in exchanging the group key results in an efficient time complexity of $O(\log_2 n)+1$ for N number of participating nodes. The computations carried out in key exchange algorithm involves simple XOR operation and modulus operation thus reducing the computational overhead on the participating nodes and thus increases the efficiency of multicast session.

5. CONCLUSION

The proposed new multicast protocol is capable of handling multicast session involving both small and large number of nodes making the protocol scalable. The solution for maintain the stability of the link established among the participating nodes is also maintained by establishing a core based mesh structure when number of nodes in the session exceeds the threshold value (th =20). The protocol also authenticates the members of the group by issuing OTP and the key exchange mechanism is also carried out in a secure manner with low computational complexity. Thus the proposed algorithm improves the robustness of multicast session and thus

improves the packet delivery ratio which in turn improves the overall efficiency of multicasting among the members of the group.

6.REFERENCES

1. Internet Engineering Task Force (IETF), Mobile Ad Hoc Networks(MANET) working group charter, http://www.ietf.org/html.charters/manet-charter.html
2. J. Jubin and J.D. Tornow, The DARPA packet radio network protocols, Proceedings of the IEEE 75(1), January 1987, pp 21–32.
3. Hani Alzaid, DongGook Park, Juan González Nieto, Colin Boyd, Ernest Foo, A Forward and Backward Secure Key Management in Wireless Sensor Networks for PCS/SCADA,SPRINGER, 2010
4. DineiFlorˆencio and Cormac Herley, One-Time Password Access to Any Server without Changing the Server, Springer-Verlag Berlin Heidelberg 2008, pp 401-420
5. LeinHarn and Changlu Lin. Authenticated Group Key Transfer Protocol Based on SecretSharing, IEEETrans.Computers; Vol.59, no.6, 2010, pp.842-846.
6. Seetha. R and R. Saravanan, A Novel Key Exchange Algorithm for Secure Group Communication, International Journal of Applied Engineering Research, Volume 9, Number 22, 2014 pp. 13911-13916.
7. Seetha. R and R. Saravanan, A Survey on Network Layer Multicast Routing Protocols for Mobile Ad Hoc Networks, IOSR Journal of Computer Engineering (IOSRJCE), Volume 6, Issue 6, Nov. - Dec. 2012, PP 27-35