JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3647-3650
https://publishoa.com
ISSN: 1309-3452

"A study of Group Key Management Protection in Non-Network"

Ph.D Scholar: - Rituraj

Subject: - Computer Science

Email. Id:- jainrituraj@yahoo.com

UNDER THE SUPERVISION OF

Dr. Manish Varshney

Dept. of Computer Science
MUIT University, Lucknow (U.P.)
Email. Id:- itsmanishvarshney@gmail.com

Received 2022 March 15; **Revised** 2022 April 20; **Accepted** 2022 May 10.

Abstract

Because of the widespread use of mobile devices and the introduction of multicast communication, significant effort has gone into establishing an optimal group key management protocol for mobile multicast systems and MANETs. For both wired and wireless networks, key management is frequently used to secure group communication. Securing group communication on wired networks is well established; but, due to member mobility and the growing number of members, a wireless network poses additional issues. They are divided into two categories: network-dependent and network-independent protocols, as well as tree-based and cluster-based key management systems.

Keyword: - Communication, Establishing, Network, Protocols.

Introduction

"Multicast technology demonstrates significant functionality that permits the efficient implementation of group communication, in which a single sender delivers a message to several receivers at the same time" (Deering, 2006). "The design of a group key management protocol (GKMP) is a core aspect of any security framework for group or multicast communication that relies on cryptographic services," says the author (Hardjono and Tsudik, 2000b). "A Group Key Management Protocol displays the personnel and procedures that govern all elements of cryptographic key management," says the author (Murray W. H, 2000). Simultaneously, it's critical that procedures for maintaining cryptographic keys are secure and meet the security goals of certain applications. It's also critical to protect multicast group applications against security threats such as monitoring sensitive communications, inserting fraudulent data traffic, changing key values, or masquerading as a multicast group member. The main concerns in group communication, according to the "Internet Engineering Task Force" (IETF), include handling cryptographic keys groups. Following that, there was

Group Communication-Related Security Issues

This thesis examines critical security challenges in group communication, such as unicast. Integrity, authentication, accessibility, and confidentiality were all concerns for group communication security service providers. When attacking a multicast transmission, the unicast enemy will carry both active and passive attacks.

- Surveillance of confidential communications
- The group session is upsetting.
- Data transmission is being blocked.

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3647-3650
https://publishoa.com
ISSN: 1309-3452

- Injecting fictitious data congestion
- Acting as if you're going to a group session
- Individuals conspiring information and forming a fictitious group session to get unlawful access; group members may have cryptographic keys and other group-related data (or information). As a result, it is critical to communicate (or send) secure data sharing information to the group members.

Group Authentication and Security

In order to provide security services in secure multicast contexts, entity authentication, data integrity, and secrecy are required. The following are some specific requirements for secure multicast group communications:

(a) A host must have its own security requirements for joining particular groups or other groups (for example, who can join the groups), multicast group communication must provide its own security services that are only accessible to authorized members, and the group manager will verify the service provided by.

- Individuals in a group confirm that the service they are receiving is from a legitimate source. Members of the group and the group managers will cross-check each other's identities.

(b) The other two options, static and dynamic, may have different requirements for dealing with group communication keys due to member departs and joins. If backward and forward secrecy is required in a dynamic approach, group keys must be re-keyed anytime there is a change in group membership.

Scalability

In general, scalability refers to a framework's (or design's) ability to scale to a larger number of hosts over a larger physical region while maintaining the same quality of service. By using a single design, you may provide important changes to all of the group members separately (All the members protected by separate key). If the group is large and/or has a very dynamic group membership, scalability challenges for secure group communication should be addressed from the beginning of any key management architecture.

MANET Key Management Schemes Overview

Key Management Schemes with Asymmetric Keys

In recent research articles, numerous key management strategies or systems for MANETs have been proposed. The underlying principle behind most public key encryption is to distribute the CA function among multiple nodes. "A secure key management technique based on threshold cryptography (t, n)." T-1 hacked servers are tolerated by the system" (Zhou and Hass, 1999). "A localised key management method in which all nodes are servers and the certificate service can be provided locally by a set of surrounding nodes." A similar technique was proposed by Yi, Naldurg, and Kravets" (Luo, Kong, and Zerfos, 2001). Their certificate service is distributed to a selection of nodes that are physically more secure and powerful than the others. 2007 (Wu and Wu) “presented a technique similar to Yi, in which server nodes form a mesh structure and an efficient ticket scheme is used." (J. Hubaux, L. Buttyan, and S. Capkun, 2001) "I examined a fully distributed technique based on the same concept as PGP." (Kravets and Yi, 2002) Provide a logical model of confidence. Their plan was to take advantage of the advantages and disadvantages of both central and entirely dispersed trust structures.

Key Management Schemes with Symmetric Keys

Review of Literature

The literature review focuses mostly on current challenges, security risks, authentication, and prior techniques used to solve inclusive problems.

The GKMP problem is a well-known issue that has been brought to light by various academics and addresses group

communication issues in wireless networking. "Due to latency and node failure, fault tolerance is a key negative in asynchronous networks," says the author (Bhargava and Madria, S. K, 2000). Failure detection and repair techniques result in the groups exchanging failure notifications on a regular basis. "In such networks, the overhead is limited by establishing a consistent ring structure with pair wise messages for detecting group communication failures," says the author (Seba, H...FTKM, 2006). Apart from that, security is the primary concern in the cloud environment. In unsecure ad hoc networks, the GKMP approach is treated as a resource-intensive protocol. Without a centralized network, the security of such a network is limited by using a key-based open network. The keys are made in such a way that they alter in accordance with the participants. "An efficient, clean, and secure three-round authenticated group key agreement system that performs well on ad hoc networks," according to the proposal (Augot et.al, 2007). "In a multicast context, an effective protocol with an algorithm." This protocol addresses the overhead difficulties by employing two solutions: the key is produced at the server during each event, and the key is multicast across all groups," according to the proposal (Pour et al, 2007). "A multilayer security and a decentralized group key management architecture that reduces overhead, as well as avoiding single point failure employing better resilience problem," according to the proposal (Huang and Medhi, 2008). Over groups, a secure roaming protocol is implemented without the use of fresh keys. Even in the event of a failure, the group key provides more security. (Cho et al, 2008) suggested a "region-based protocol" that divides groups into sub-groups and determines the best method to improve network performance. Using trade, this strategy decreases network traffic overhead between inter-regional and intra-regional overheads" When compared to region-based protocols, non-region-based protocols perform poorly. Furthermore, (Cho and Chen, 2008) proposed a "region-based approach combined with an intrusion detection algorithm that effectively removes threats." This method selects the nodes with the greatest number of votes in a given region." "It's then loaded with an intrusion detection algorithm that diagnoses the other nodes in the vicinity."

Study of the Objectives

The main goal of this study is to develop a security protocol for multicast environments in order to protect group (or multicast) communication in wireless networks. The following are the primary research goals:

- To identify ideas and improve authentication, membership changes, and rekeying efficiency in a cloud context.
- To create a useful mechanism for user privacy protection, such as encrypting data saved in the cloud using a digital signature and the R-CP algorithm.
- To compare the proposed design's productivity to that of existing designs in terms of authentication, low rekey efficiency, suitable membership change, and storage and communication overhead.

The Purpose of Research

Group-based applications have recently garnered a lot of traction. The following are some of them:

- Multimedia presentations, such as video, audio, and on-demand chat or teleconferencing.
- Information transmission services, such as the stock market, quotes, breaking news, or software upgrades, are examples of push technologies.
- Pay-per-view (PPV) channels, for example, are satellite television distribution services.
- Connected online systems, such as virtual classrooms.

This thesis was particularly concerned with the security arrangements for group communication.

Research of Methodology

The purpose of this thesis is to establish a group key management mechanism (GKMP). We believe that this research will add to our understanding of secure group communications in wireless networks in the cloud:

JOURNAL OF ALGEBRAIC STATISTICS
Volume 13, No. 3, 2022, p. 3647-3650
https://publishoa.com
ISSN: 1309-3452

(1) In a wireless cloud context, this research provides reduced overhead and a more powerful security mechanism.

(2) This starts a group key management protocol that spans many protocols in small and large groups for high-quality scalability in networking designs.

(3) This study is focused on a group key management system for cloud-based wireless networks. The core GKMP is described in detail in this thesis.

This study conducts a fundamental evaluation of the protocol's security, functionality, and performance

Conclusion

Security and overhead concerns are consistently addressed by the recommended region-based clustering method. Other conventional methods are outperformed by the clusters over HS idea and the addition of projective geometry encryption. This is due to the fact that the suggested approach makes use of the HS concept, whereas other conventional ways use a tree-based approach. The suggested approach has a simple computational structure. On the other hand, the operation has a stronger encryption than conventional methods.

Reference

1. Harney, H. and Muckenhirn, C. (1997). Group Key Management Protocol (GKMP) specification. RFC 2093
2. Hillebrand, F. (2002). GSM and UMTS: The Creation o Global Mobile Communication. John Wiley & Sons, Ltd.
3. Hinden, R. and Deering, S. (2006). IP Version 6 Addressing Architecture. RFC 4291. [37]. Hubaux, J., Buttyan, L., and Capkun, S. (2001). The Quest for Security in Mobile Ad
4. Hoc Networks, In Proc. of the ACM Symposium on Mobile Ad Hoc Networking & Computing (MobiHoc 2001).