International Journal On Engineering Technology and Sciences – IJETS
ISSN(P): 2349-3968, ISSN (O): 2349-3976
Volume VII, Issue V, MAY - 2020

CONCEPT OF MANAGING ID AND AGREEMENT OF GROUP ID FOR FAST TRANSMISSION TO THE DISTANT GROUPS

M. Anisha Vergin,
Assistant Professor,
Dept., of Computer Science and Engineering, Lourdes Mount College of Engineering and Technology, Mullanganavilai, KK., District, Mail Id: anisha.vergin@gmail.com

Abstract --

In newly concept of emerging networks, the secure and efficient broadcasting to a distant supportive group is one of the major problems. In this paper, an approach of a novel ID management is proposed to solve this problem. The new approach is a cross of existing problems in encoding and agreement for group ID. Each node will have a public/secret ID pair. Public/secret ID of the node, a sender can securely broadcast to any group by seeing that which is not anonymous. In the proposed method, it is to enable send and leave broadcast to distant cooperative groups. If the non-aimed members conspire, they cannot be able to extract any information from the transmitted messages. The proposed scheme is used to provides the efficient member of deletion/addition, flexible re ID strategies and is also well-organized in terms of communication.

Keywords — Access control, ad hoc networks, cooperative computing, Information security, ID management, distant group, mobile ad hoc networks, wireless mesh networks and vehicular ad hoc networks.

I. INTRODUCTION

In the innovative merging networks, the broadcasting message to distant obliging groups using encrypted communication is necessary. In distant group the communication arises in WMNs, MANETs, VANETs, etc. Wireless mesh networks (WMNs) are vigorously self-organized with the nodes in the network automatically establishing an ad hoc network and maintaining the mesh connectivity. It is a multihop layered wireless network. Wireless mesh networks have two different types of nodes, such as mesh routers and mesh clients. The ability of routing for a gateway/bridge purposes a mesh router is created for additional routing purposes to support mesh networking. In the multi-hop communications also, the same exposure can be attained by a mesh router with a low transmission power.

To improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies.

The system MANET is created by wireless mobile nodes, in which the nodes have the characteristics such as wireless transmission and network management. MANETs are introduced for providing operative networking-based system and smoothing data between mobile devices without a fixed infrastructure. The audial/audiovisual conference from one-to-many data dissemination in combat zone rescue scenarios is in the MANET applications.

VANETs are deployed in the near future. A VANET have OBUs (on-board units) which are fixed in the vehicles and are serving as a mobile computing node and RSUs (roadside units). The VANETs are act as the information gathering organizations which are situated in the perilous points on the road. In the wireless communication range in the roads the mobile vehicles form many groups, and by the roadside infrastructures, the vehicles can access other networks. For improving the traffic safety VANETs are designed and the other aim is for providing value-added facilities to the vehicles.

In the case of group communication, the rectified solution of the authorization of a sender to send the messages securely to a distant cooperative group which is considered as a main problem must meet several restraints. Firstly, the sender will be located in a distant place and it will be in dynamic state. Secondly, the transmission may have fusion of many different types of networks which includes open networks that are insecured before the messages reaches the projected recipients. Thirdly, the messages send from the group nodes to the sender may be in limited range. It is very difficult to re-arrange a fully trusted third party for securing the communication messages because the sender will choose the intended recipients. The features of the mentioned limits are the cooperative group nodes are and the communication between them is local and in efficient way. This paper has the features to simplify the remote access control of group communications without be sure of a fully trusted third party.

A. Contribution

In this paper includes three facets. The agreement of group ID provides an efficient way is to lock the group-to-group communication level, but for an isolated sender, the requestor asked to stay online with the group members by the provider to negotiate a secret session ID before communicating with any encrypted mode secret messages for multiple rounds of interactions. The delinquent of securing transmission to distant groups is formalized, the main fundamental is to make a one-to-many communication in secure and efficient manner under certain circumstances. This is not possible for an isolated sender whose time zone will be varies. This is the further depreciated if the sender is in the form of mobile or else in dynamic state. Transmission encrypting enables the external senders to transmit the messages to a predetermined group with non-supportive members and without necessitating the sender to interact with the destinations before sending the encrypted type or most secret messages, but it be sure of on a centralized ID server to engender and scatter the secret IDs for each node in the group. This shows that: 1) before a confidential transmission channel is established, the ID server should raise the intimate unicast channels to each probable receiver; and 2) the secret ID of each destination of the ID server has a point that can read all the messages and that will be copiously trusted by anyone of the sender and the group members.

B. Paper Organization

C.

The respite of this paper is ordered as follows. Section II has the system architecture and Section III contains a brief explanation about the proposed scheme of ID management. Section IV consists of created modules. Section V is about Results and finally the Section VI has the conclusion about this paper.

II. SYSTEM ARCHITECTURE

The potential destinations which are connected together with local connections in good arrangement. Through communication infrastructures, they can also connect to the heterogeneous network. Every service provider has a public/secret ID pair. The public ID will be authenticated by the credential authentication method and the secret ID is known by the requestor not even known or anonymous to the credential authority authenticator.

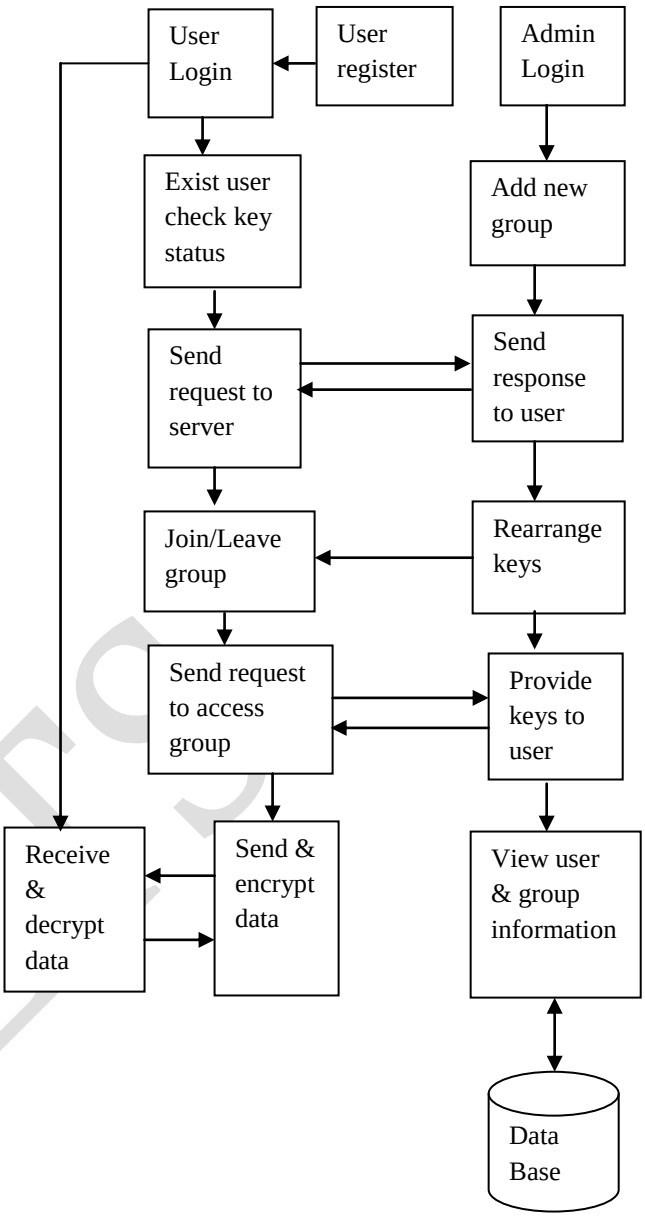

Fig .1. System Architecture

The sender validates it's authentication by checking its obtained certificate from the certificate authority the sender will takes the receiver's public ID. Where there is no direct communication between the destinations and the sender.

III. ID MANAGEMENT AND ID DISTRIBUTION

A. Proposed Approach

The proposed system of ID management includes both the broadcast encryption systems and group ID management systems.

ID Generation:

The ID generation limitations include the separate node number and the total number of members existed in the group. Thus, public or secret ID duo and the session IDs are engendered. After the IDs are engendered, the scattering of IDs is carried out for the communication of messages.

Encryption*:*

Immediately when the IDs are scattered to the group, the members of the group can start to diffuse the messages. The sender will encode the message and then forwarded it to the destination node or receiver. To encode the data, the sender will repossess the receiver's public ID from the permitted authority; it checks and validates the permission.

Decryption:

The receiver will decrypt the data by using the session ID which is distributed by the sender.

B. Member Organization

The Management of ID (i.e., the agreement of group ID or transmission encoding) includes the methods for forming the users in a tree structure. By the major least bits the users formed the chain of their private public IDs, and then a ring shape is formed by closing the chain with the sender node or lump of network. It is favorable to organize them in a chain shape tree structure and then the sender will close the chain by forming a cogent ring-shaped structure.

C. Member Deletion/Addition

In the existing agreement system of group ID to obliterate a group member or join up a new member that includes several rounds of broadcasting among the members which requires the sender to broadcast securely to the destinating group set. In the upcoming proposed system, it is meek for a requestor to discount a member or network lump from the group by deleting the public ID of the particular member or network lump from the chain of public ID. For joining up a user as the new member of the group or to the node by inserting that user's public ID in the proper position in the chain of the destinations. After a member gets deleted its public ID will be deleted from the certificate authority. Thus, deleted member cannot read the previous transmission. After the completion of deletion/addition process, a new ring-shaped structure is formed.

IV. MODULES

The proposed approach includes the following modules: User authentication, Group creation and provide IDs, join group and leave the group, re schedule of ID and storage.

A. User Authentication

New node can join to the group and able to transfer messages. Once a member is added to the group its public/secret ID will be created and the public ID is sent to the certificate authority for the checking purpose.

B. Group Creation and Provide IDs

Generate a group to join the nodes for broadcast transmission. Once a group is formed nodes will join the particular group. Each node should have a public or secret ID duo and the IDs are corroborated and validated by the credential authority. Only the public IDs are known by the certificate authority but the secret ID is known and kept only by the receiver. The certificate authority validates the ID by checking its certificate authentication. The destination point's public ID will be recapture by the sender from the credential authority to jerk the data transmission. Then the session ID will be created and sent by the sender. Next the sender will encrypt the message and also it sends the secret session ID to the recipient or receiver for occurring a secure data transmission. The receiver will decrypt or decode the session ID send by the sender which is placed in the header and also the receiver will be encrypted or encoded message.

C. Join and Leave the group

A new member can also be able to join the group and also, can able to sends its public ID to the certificate authority, it authenticates by checking its certificate. Also, a member can get deleted from the group; once a member is deleted its public ID will also get deleted. Deleted member cannot read the group transmission messages. Joining and leaving a member from the group is easier in the proposed tactic.

D. Re scheduling of ID and storage

Every member in the group has its own public or secret ID for secure data transmission. The IDs will be updated routinely by fetching its group name from the isolated group. The broadcasting of data to the distant group is faster in the proposed approach using the novel ID management tactic.

V. EXPERIMENTAL RESULTS

In the proposed approach a new ID management system is used for secure communication. A new member can join and also existing member can get deleted from the group. The IDs are updated automatically by using the group member. The IDs are distributed before starting the transmissions. Group is created to join the node and the

sender will encrypt the message and the session ID is placed in the header. The receiver will decrypt the ID and also the encrypted message. In the receiver side the sender node, transmission times are displayed.

VI. CONCLUSION

Here the conclusion will be as a new ID management tactic scheme is proposed to enable send data and leave the messages or packets without trusting on a fully trusted other node to the distant cooperative groups, the proposed approach provides efficient method of member deletion/addition, flexible re scheduling of ID strategies and also efficient in the terms of computation and communication.

REFERENCES

[1] Y. Qian, K. LuR. Q. Hu, H.-H. Chen, "Security model for group-oriented computing," IEEE Transaction *Vehicle Technology*., vol. 58, no. 1, pg No: 398–408, Jan 2009.

[2] C. Gentry and B. Waters, "Adaptive security in broadcasting encryption systems," *Advanced Cryptography*., volume 5479, EUROCRYPT' 09, pg no: 171–188, 2009.

[3] M. Gouda, and S. Lam, "Secure group communications using ID," *IEEE Transaction Network*, volume 8, no. 1, pg no: 16–30, Feb 2000.

[4] D. Halevi and A. Shamir, "The LSD broadcasting encryption method," volume 2442, pg no: 47–60, 2002.

[5] N.S. Jo, M.-H. Kim, and E. S. Yoo, "Dropping the combined chain schemes for broadcasting encrypted messages," *IEEE Transaction on Information Theory*, volume-54, no. 11, pg no: 5155–5171, November 2008.

[6] B. Waters, C. Gentry, "Avoidance of Mobbing in broadcast encryption with short ciphertexts and private IDs," *Advanced Cryptography method*, volume 3621, pg no: 258–275, 2005.

[7] M. Barmaster and Y. Desmid, "A secure and efficient conference ID distribution system," *Advanced Cryptography*, volume: 950, EUROCRYPT'94, LNCS, pg no: 275–286, 1995.

[8] M. Nao and B. Pikas, "Efficient trace to revoke methods," in *Proc. 4th FC*, 2001, volume 1962, pg no: 1–20.

[9] M. Weiner, "Dynamic peer groups using ID agreement," *IEEE Transaction*, volume 11, no. 8, pg no: 769–780, August 2000.

[10] A. Menezes, "Pairing-based cryptography at high security levels," *Cryptography Coding*, vol. 3796, pp. 13–36, 2005.

AUTHORS BIOGRAPHY

M. Anisha Vergin, currently working as Assistant Professor in Lourdes Mount College of Engineering and Technology, Mullanganavilai. Her Research area includes Network Security and Cryptography.