International Journal Of Scientific Research And Education
||Volume||2||Issue||10||Pages-2002-2009||October-2014|| ISSN (e): 2321-7545
Website: http://ijsae.in

Real Time Data Transmission to Remote Client Groups with Cryptographic Techniques

Authors
P.V.S. Srinivas[1], Y.V.S.V.Sarma[2]
[1]Professor, Department of CSE, TKR College of Engineering & Technology, Hyderabad, India.
[2]PG Scholar, Department of CSE, TKR College of Engineering & Technology, Hyderabad, India.
Email- [1]pvssrinivas23@gmail.com [2]yvsvarun@gmail.com

ABSTRACT

Mobile Ad-hoc Networks (MANETs) allow wireless mobile nodes to form a network without requiring a fixed infrastructure for facilitating data exchange between these nodes for an effective networking system issues into account. In various types of adhoc networks, a problem arises in group-oriented communication with access control. In this paper, we overcome this drawback by proposing a group key agreement based broadcast encryption, where this scheme incorporates the up-to-date definitions of group key agreement and public key broadcast encryption. The implementation of group key agreement protocols innovatively brought up the broadcast encryption in an efficient way. We focus on the confidentiality of the session key by modeling a key encapsulation mechanism in which a sender can send a short secret session key to the intended receivers whereas long messages can also be encrypted by using symmetric encryption algorithm.

Keywords- *Group key agreement, Broad cast based encryption, GKA protocols, and multihop wireless mesh networks.*

I. INTRODUCTION

A multihop packet based wireless network composed of a set of mobile nodes that can communicate and move at the same time, without using any kind of fixed wired infrastructure is referred to MANET (Mobile Ad hoc Network). MANET is in fact self organizing and adaptive networks that can be formed and deformed on-the-fly without the need of any centralized administration. By means of mature components from previous work on experimental reactive and proactive protocols, the WG will expand two Standards track routing protocol specifications. They are namely Reactive MANET Protocol (RMP) and Proactive MANET Protocol(PMP) . The other two types of routing protocols are Table-Driven Routing Protocols and Source-Initiated On-Demand Routing Protocols. Here, in wireless communication networks the devices can receive transmitted messages as the communication is broadcast and efforts are to be put to provide secure group communications because it plays an essential role in MANETs. The main problem identified in group communication is to enable the sender to securely transmit messages to a remote cooperative group[1]. So, to overcome this drawback, the sender can be remote or dynamic also. Then next, before reaching the intended recipients, the transmission may cross various networks including open insecure networks [2]. Finally, the communication is limited between the group members and the sender. It is very hard to resort to a fully trusted third party to secure the communication and keeping in view of these mitigating features without relying on a fully trusted third party and to facilitate remote access control of these communications[4].

II. RELATED WORK

The multihop wireless mesh networks (WMNs) are discovering eternally increasing recognition as a feasible and effectual resolution to pervasive broadband internet access. This scheme addresses the defense of WMNs, which is a key obstruction to large extent use of WMNs. Attack resilient security architecture provides capable mutual authentication and key agreement among a user and a serving WMN domain, and is designed to be flexible to an ample variety of attacks[3]. Safety measures and isolation issues are of mainly unease in approaching the achievement of WMNs for their large exploitation in addition to support service oriented applications. Regardless of the need, some degree of safety measures has been conducted in the direction of isolation protection in WMNs which motivate us to build up PEACE, a new privacy enhanced yet accountable security framework customized for WMNs. It enforces exacting user access control to handle equally with free riders and malevolent users by using short group signature variation [5]. It also provides refined user confidentiality defense in opposition to both adversaries and a range of network entities. In mobile ad hoc networks (MANETs), various applications involve in group oriented computing along with a great number of nodes in an adversarial background. To organize these helpful applications, a secure multicast service should be provided to proficiently and securely swap over data among nodes. As a major aspect, a pyramidal security model consists a set of hierarchical security groups and multicast groups to facilitate data exchange among mobile devices without any support of wireless access points. With this service, the concerto of groups is recognized by the forming of group keys. Vehicular ad hoc networks (VANETs) are mainly developed to advance the traffic protection and competence [4]. A privacy preserving system is proposed that guarantees message reliability in vehicle to vehicle interactions. Vehicle isolation is considered as long as a vehicle do not effort to back the similar message more than one time The substantiation of legitimate vehicle to vehicle communication is accelerated by group message processing methods. For secure intra group communication, group key agreement provides an efficient solution which is explained in this way. For a remote sender, the sender has to stay online with the group members for multiple rounds of interactions before transferring secret information [6].But as this case is not succeeded. due to some drawbacks in it, a broadcast to non-cooperative members of a present group without requiring the sender to interact with the receivers before transmitting secret information . A centralized key server will be present to generate and distribute secret key for each group member[7].

III. SYSTEM DESIGN

To finish the transmission in an efficient as well as in secure way, the sender must be enabled to meet the constraints .The challenging tasks and drawbacks of the previous scenarios are given as, deployment of key generation authority, limitation of communication from the receivers and sender as well as receiver parties both must be dynamic in adhoc communication[6].To overcome these drawbacks our contribution lead to provide efficient broadcast channels and a public key infrastructure is also made available to authenticate the receivers and also senders. When we speak about the initial mechanism, with efficient local connections, the receivers are connected. Here, each receiver will have a public/secret key pair [3]. The certificate authority certifies the public key and the secret key is known only to the receiver [2].From the certificate authority, the remote sender can retrieve the public key of receiver and checks its certificate and then after completes the validation and authentication processes. From now, the senders can send secret information to the receivers. The group key agreement based broadcast encryption incorporates the up-to-date definitions of group key agreement [9].The sender can encrypt the message under the session key by the mechanism of session key encapsulation, so that the decryption process can be done by intended receivers. The proposed key management system is specified by algorithms which process following features [5].

The Key generation algorithm is used to generate public/private key pair. Verification and authentication procedures are followed and done by sender.

Next comes up with encryption procedures, which is run by sender who knows the public key of the receiver. This algorithm incorporates the functionality in the initial mechanism.

(iii) Finally, the decryption algorithm is run by the intended receivers to extract the secret information send by the sender. This algorithm incorporates the traditional group key agreement method.

In modern approach, the third party is not fully trusted and only trusted partially.

This procedure is implemented by PKI (Public Key Infrastructure) in open networks.

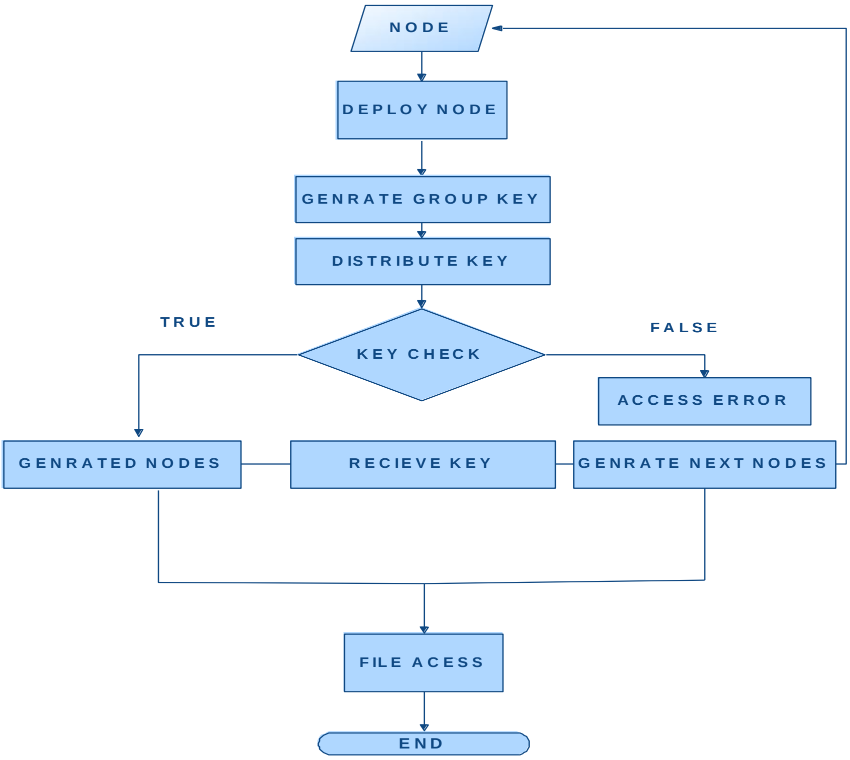

Fig 1: Depicts the flow of proposed system

Presumably, new key management paradigm requires a sender to know the keys of the receivers. But, this concept in traditional way needs a communication from receivers to the sender. In the proposed model, from a third party, the sender need to obtain the receiver's public key by having no direct contact between the sender and receiver parties. This provides feasibility for a remote sender and also assures secure transmission to remote cooperative groups. Efficient encryption and short cipher-text is the major requirement for the proposed model. Now, we discuss about the secrecy of a group key agreement based broadcast encryption scheme, which is modeled as key encapsulation mechanism, through which the sender can send a short secret session key possibly and also even long messages using the another algorithm namely, symmetric encryption algorithm(AES is preferable).The proposed model is collusion-resistant against adaptive attacks and also incorporates GKA protocols efficiently[6]. The KeyGen, Encryption and Decryption are the common procedures for the proposed system and the functionality differs between the traditional and modern approaches. Let us see the procedure of the algorithms, how the sender runs in a step-wise manner.

Random selection and computation.

Public group encryption key extraction

Secret Session key computation

Header Broadcasting

With the help of the session key, the receiver can read the messages.

IV. SYSTEM IMPLEMENTATION

4.1 Broadcast Encryption:

Organizing the users in a tree-based structure is the vital functionality provided by this scheme. In order to organize them in a chain, the sender will be used to close the chain to form a logical ring. In this chain, if the senders change, then the receivers has to communicate with other receivers during decryption process. The chain is formed by ordering the users unique public keys by forming in a ring format[4]. The certificate authority forms the list of users and corresponding public keys in the same order. With this approach, no specific sorting efforts are required by sender side.

4.2 Proposed Scheme:

Here, in this scheme, we focus on the different aspects like member deletion, addition and group partition and merging also. In the proposed scheme, the sender can exclude a group member by deleting the public key of the member from chain is available at free of cost. A logical public-key ring automatically forms after the deletion or addition of a member from the chain. If this happens, then the sender and other receivers have to notice the changes to the encryption and also for decryption procedures. In member addition process, the sender has to retrieve the public key of the member and insert this key in to the public key chain of the current receiver set. The modifications must be done in encryption as well as in decryption procedures also. By performing the same member addition operation, the sender can merge any 2 receiver sets in to single group[10]. The same process is done for member deletion operation also.

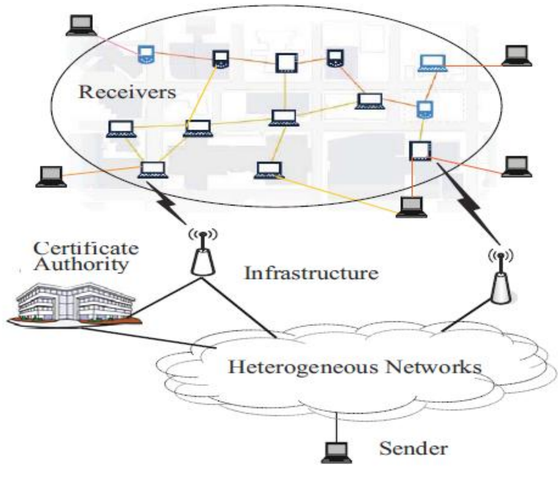

Fig 2: Overview of System Design

4.3 Key Update Mechanism:

The mechanism involves in 3 levels of key update strategies. The first level, session key update will update the session key, that is used to encrypt the digital contents to the receivers and for every session it gets expired. For this process, the sender will first select a new value randomly and computes the session key and broadcasts it to the receivers. During this process, there is no need of any communication between both the parties. The second level, which is used to update the secret decryption key called as group decryption key update. The third level is used to update the secret key namely, long-term secret key update. This is required when the user key gets expired. Again the user requires the key, and then has to register for new public key at certificate authority. The same procedures of encryption and decryption are applicable here also.

V. SYSTEM PERFORMANCE AND EVALUATION

In group decryption, the time delay is very low and the cost of encryption to group linearly grows with the number of receivers. The delay incurred is slower than the growth of network delay. In an ad hoc way, the sender can transmit to the remote group that result in reducing the number of communication rounds to cope with member changes in key management protocols designed for MANETs. The network time for member addition and deletion operations are similar and in this approach, the remote sender can stay online with the receivers. One more important factor is we do not require fully trusted key server.

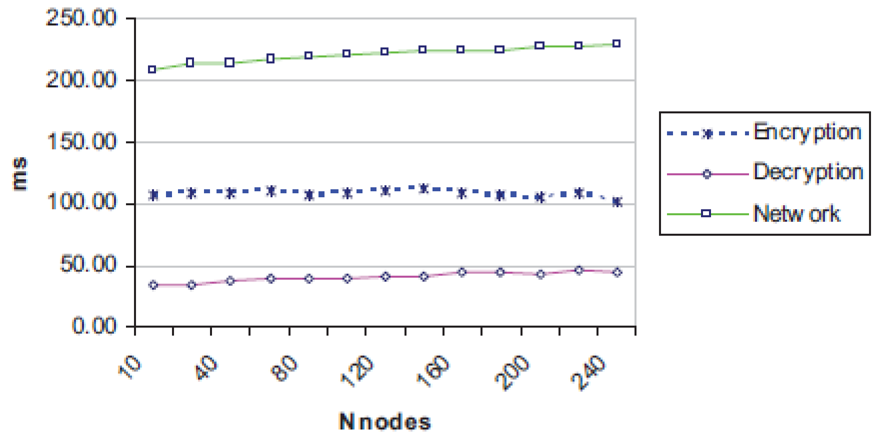

Fig 3: Cost of Member Deletion

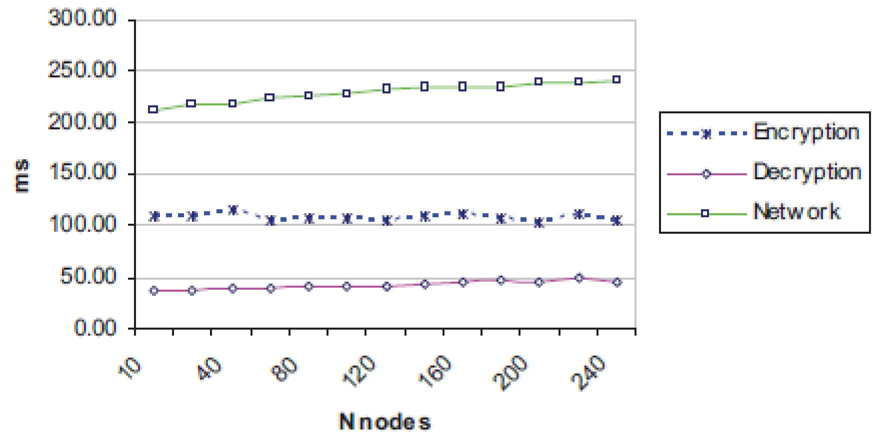

Fig 4: Cost of Member Addition

VI. CONCLUSION AND FUTURE SCOPE

In terms of computational and communication wise the new key management is efficient and enable send-and-leave broadcasts to remote cooperative groups. The broadcast encryption scheme functionality and its organizing help to form a logical ring when the chain gets closed. In this scheme, the sorting efforts are reduced. The key update mechanism results in effective way by updating the secret, session keys and broadcasting to the receivers.Here in this proposed scheme updating the long-term secret key of a member causes more overhead than updating the session key or group decryption key, although the long-term secret key update process is efficient. The unwanted burden can be reduced by changing the long-term secret key for little number of times only.

REFERENCES

[1] Y. Zhang and Y. Fang, "ARSA: An attack-resilient security architecture for multi-hop wireless mesh networks," *IEEE J. Sel. Areas Commun.*, vol. 24, no. 10, pp. 1916–1928, Oct. 2006.

[2] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 21, no. 2, pp. 203–215, Feb. 2010.

[3] B. Rong, H.-H. Chen, Y. Qian, K. Lu, R. Q. Hu, and S. Guizani, "A pyramidal security model for large-scale group-oriented computing in mobile ad hoc networks: The key management study," *IEEE Trans. Veh. Technol.*, vol. 58, no. 1, pp. 398–408, Jan. 2009.

[4] P. V. S. Srinivas, "An innovative approach for maximizing throughput in wireless networks," Advances in Computational Sciences and Technology(ACST),vol. 2,Issue: 2,*ISSN*: 0972-6107, pp. 127-130.

[5] M. Burmester and Y. Desmedt, "A secure and efficient conference key distribution system," *Adv. Cryptol.*, vol. 950, EUROCRYPT'94, LNCS, pp. 275–286, 1995.

[6] M. Steiner, G. Tsudik, and M. Waidner, "Key agreement in dynamic peer groups," *IEEE Trans. Parallel Distrib. Syst.*, vol. 11, no. 8, pp. 769–780, Aug. 2000.

[7] A. Sherman and D. McGrew, "Key establishment in large dynamic groups using one-way function trees," *IEEE Trans. Softw. Eng.*, vol. 29, no. 5, pp. 444–458, May 2003.

[8] Y. Kim, A. Perrig, and G. Tsudik, "Tree-based group key agreement," *Trans. Inf. Syst. Security*, vol. 7, no. 1, pp. 60–96, Feb. 2004.

[9] P. P. C. Lee, J. C. S. Lui, and D. K. Y. Yau, "Distributed collaborative key agreement and authentication protocols for dynamic peer groups," *IEEE/ACM Trans. Netw.*, vol. 14, no. 2, pp. 263–276, Apr. 2006.

[10] W. Yu, Y. Sun, and K. J. R. Liu, “Optimizing the rekeying cost for contributory group key agreement schemes,” *IEEE Trans. Depend. Secure Comput.*, vol. 4, no. 3, pp. 228–242, Jul.–Sep. 2007.

[11] M. Abdalla, Y. Shavitt, and A. Wool, “Key management for restricted multicast using broadcast encryption,” *IEEE/ACM Trans. Netw.*, vol. 8, no. 4, pp. 443–454, Aug. 2000.

[12] Y.-M. Huang, C.-H. Yeh, T.-I. Wang, and H.-C. Chao, “Constructing secure group communication over wireless ad hoc networks based on a virtual subnet model,” *IEEE Wireless Commun.*, vol. 14, no. 5, pp. 71–75, Oct. 2007.