ISSN:0975-9646

Improving security By Quantum Cryptography in P2P Reputation Management in Distributed Identities and Decentralized Recommendation Chains

V V Murali Babu Polukonda, A Harish

Vignan's Institute of Information Technology Duvada
Visakhapatnam dist, Andhra Pradesh, India.

Abstract—Peer-to-peer (P2P) networks are vulnerable to peers who cheat, propagate malicious code, leech on the network, or simply do not cooperate. consider several distributed collaborative key agreement and authentication protocols for dynamic peer groups. There are several important characteristics which make this problem different from traditional secure group communication. Authentication focuses on the security improvement, while implementation realizes the interval-based algorithms in real network settings. Our work provides a fundamental understanding about establishing a group key via a distributed and collaborative approach for a dynamic peer group. In this paper presents quantum key distribution protocols (QKDPs) to safeguard security in large p2p networks, using in new directions in classical cryptography and quantum cryptography. Two mediator protocols, one with implicit user authentication and the other with explicit mutual authentication, are proposed to demonstrate the merits of the new combination, which include the following: 1) security against such attacks as man-in-the-middle, eavesdropping and replay, 2) efficiency is improved as the proposed protocols
Contain the fewest number of communication rounds among existing QKDPs, and 3) two parties can share and use a long-term secret (repeatedly). To prove the security of the proposed schemes, this work also presents a new primitive called the Unbiased-Chosen Basis (UCB) assumption.

Index Terms: Peer-to-peer networks, distributed systems, security.

INTRODUCTION

All peers in the P2P network are identified by identity certificates (aka identity). The reputation of a given peer is attached to its identity. The identity certificates are generated using self-certification, and all peers maintain their own (and hence trusted) certificate authority which issues the identity certificate(s) to the peer. Each peer owns the reputation information pertaining to all its past transactions2 with other peers in the network, and stores it locally. The peers are connected with insecure communication channels. As the peers are likely to have conflicting interests, a source of motivation is needed to reduce the number of leechers. Leechers are peers who derive benefit from the system without contributing to the system. The rogue peers can also spread malware in the network (when other peers download content from them). Finally, peers need a mechanism to judge the quality of the content before making Go/No-Go decision in transactions and thereby develop trust relationships with other peers. KEY distribution protocols are used to facilitate sharing secret session keys between users on communication networks. By using these shared session keys, secure communication is possible on insecure public networks. However, various security problems exist in poorly designed key distribution protocols; for example, a malicious attacker may derive the session key from the key distribution process. A legitimate participant cannot ensure that the received session key is correct or fresh and a legitimate participant cannot confirm the identity of the other participant. Designing secure key distribution protocols in communication security is a top priority. In some key distribution protocols, two users obtain a shared session key via a trusted center (TC). Since three parties (two users and one TC) are involved in session key negotiations, these protocols are called three-party key distribution protocols, as in contrast with two-party protocols where only the sender and receiver are involved in session key negotiations. In classical cryptography, three-party key distribution protocols utilize challenge response mechanisms or timestamps. However, challenge response mechanisms require at least two communication rounds between the TC and participants, and the timestamp approach needs the assumption of clock synchronization which is not practical in distributed systems (due to the unpredictable nature of network delays and potential hostile attacks) . Furthermore, classical cryptography cannot detect the existence of passive attacks such as eavesdropping. On the contrary, a quantum channel eliminates eavesdropping, and, therefore, replay attacks. This fact can then be used to reduce the number of rounds of other protocols based on challenge-response mechanisms to a trusted center (and not only three-party authenticated key distribution protocols).

In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication. Previously proposed QKDPs are the theoretical design, security proof and physical implementation. Three important theoretical designs have been proposed Bennett and Brassard employed the uncertainty of quantum measurement1 and four qubit states to distribute a session key securely between legitimate participants. Bennett utilized two no

orthogonal qubit states to establish a session key between legitimate users. Ekert presented a QKDP based on Einstein-Podolsky- Rosen (EPR) pairs, which requires quantum memories to preserve qubits of legitimate users. Although, allow legitimate participants to establish a session key without initially sharing secret keys and do not need a TC, their security is based on the assumption of well authenticated participants. In other words, without this assumption, these protocols can suffer man-in-the-middle attacks. Hwang et al. proposed a modified quantum cryptography protocol that requires every pair of participants to preshare a secret key (a similar idea that is this work) for measuring bases selection. However, the participants have to perform public discussions to verify session key correctness. A three-party QKDP proposed in requires that the TC and each participant preshare a sequence of EPR pairs rather than a secret key. Consequently, EPR pairs are measured and consumed, and need to be reconstructed by the TC and a participant after one QKDP execution. **Benefits of Three Party Authentications for key Distributed Protocol using Implicit and Explicit Quantum Cryptography** is to used to verify the session key from trusted center and sender which improve key verification and secure the communication. Also identify the security threads in session key verification. Another advantage of this project is to avoid the network noise in message transmission by identifying the size of bytes transmitted over the network from sender to receiver and remove the extra byte content received from network

PROPOSED SYSTEM:

In quantum cryptography, quantum key distribution protocols (QKDPs) employ quantum mechanisms to distribute session keys and public discussions to check for eavesdroppers and verify the correctness of a session key. However, public discussions require additional communication rounds between a sender and receiver and cost precious qubits. By contrast, classical cryptography provides convenient techniques that enable efficient key verification and user authentication. We have two types of Quantum Key Distribution Protocol.

1. The Proposed 3QKDPMA

This section describes the details of the 3AQKDP by using the notations defined in previous sections. Here, we assume that every participant shares a secret key with the TC in advance either by direct contact or by other ways.The proposed 3QKDPMA can be divided into two phases: the Setup Phase and the Key Distribution Phase. In the Setup Phase, user's preshare secret keys with the TC and agree to select polarization bases of qubits based on the preshared secret key. The Key Distribution Phase describes how Alice and Bob could share the session key with the assistance of TC and achieve the explicit user authentication.

Problem Formulation

This work presents combination of classical cryptography (existing) and quantum cryptography (proposed).Two three-party QKDPs, one with implicit user authentication and the other with explicit mutual authentication which is used to make authentication using quantum mechanism. In classical cryptography provides convenient techniques that enable efficient key verification and user authentication but it is not identify eavesdropping. Here, the enhanced key distribution protocol using classical and quantum cryptography will improve the security and authentication

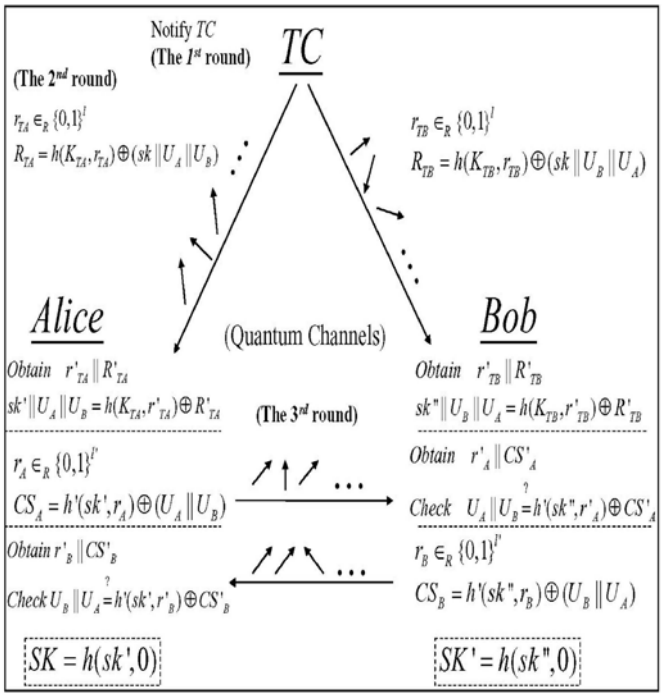

Fig1: Key Distribution Phase

SYSTEM DESIGN

Design Overview

1. Sender Module

a. Secret key Authentication

The sender give the secret key to the trusted center, then the TC will verify the secret and authenticate to the corresponding sender and get the session key from TC or else TC not allow the user transmission

b. Encryption

The message is encrypted by the received session key and appends the qubit with that encrypted message, then transmit the whole information to the corresponding receiver.

2. Trusted Center

a.Secret Key Verification

Verify the secret key received from the user and authenticate the corresponding user for secure transmission.

b.Session Key Generation

It is a shared secret key which is used to for encryption and decryption. The size of session key is 8 bits. This session key is generated from pseudo random prime number and exponential value of random number

c.Qubit Generation

To get secret key and random string, then convert into hex-code and then convert it into binary, find the least bit of the two binary values and get the quantum bit of 0 and 1.

To generate the quantum key using the qubit and session key which depends on the qubit combinations, such us?

i. If the value is 0 and 0, then $1/\sqrt{2}(p[0] + p[1])$.
ii. If the value is 1 and 0, then $1/\sqrt{2}(p[0] - p[1])$.
iii. If the value is 0 and 1, then p[0].
iv. If the value is 1 and 1, then p[1].

d.Hashing

It's a technique to encrypt the session key by using the master key and store all the values to TC storage

e.Key Distribution

It distribute the original session key and qubit to the sender for encrypting the message. Also it distribute the key and qubit to the corresponding receiver to decrypt the received messages

3. Receiver Module

a.Secret key Authentication

It receive the encrypted message with hashed session key and qubit, then verify the qubit with TC and generate the master key and reverse the hash the session key and also reverse hash the session key from sender then compare the session key which improve the key authentication

b.Decryption

Then finally decrypt the message using session key and show it to the user

CRYPTOGRAPHY

Cryptography is the process of protecting information by transforming it into an unreadable format, called cipher text. Only those who possess a secret key can decrypt the message into text. Encryption is the process of conversion of original data (called plain text) into unintelligible form by means of reversible translation ie based on translation table or algorithm, which is also called enciphering. Decryption is the process of translation of encrypted text (called cipher text) into original data (called plain text), which is also called deciphering. Cryptography systems can be broadly classified into symmetric key systems in which both the sender and recipient use a single key for encryption and decryption, and public key systems that use two keys, a public key known to everyone and a private key that only the recipient of messages uses. Each of this system make use of a algorithm for encryption and decryption in which sender make use a key for encryption of a plain text to cipher text and receiver make use of key used by sender to decrypt the cipher text to plain text this process is called as symmetric key crypto graphic algorithm. Example for symmetric key encryption algorithms are data encryption standard (DES) & blowfish. In public key encryption algorithm the sender encrypt the plain text by using the public key of receiver, the receiver decrypt the cipher text by using own private key. Example for public key encryption algorithms are Elliptic Curve Cryptograph (ECC) & RSA.

Cryptography plays a major role in the security aspects of multicasting. For example, consider stock data distribution group, which distributes stock information to a set of users around the world. It is obvious that only those who have subscribed to the service should get the stock data information. But the set of users is not static. New customers joining the group should receive information immediately but should not receive the information that was released prior to their joining. Similarly, if customers leave the group, they should not receive any further information.

Authentication:

Authenticity means that when a user receives a message, it is assured about the identity of the sender. The authenticity requirement can be translated in the context of secure multicast into two requirements on key and data distribution. **Key authenticity:** only the center can generate a session key. **Data authenticity:** the users can distinguish among the data sent by the center and the malicious data sent by an attacker.

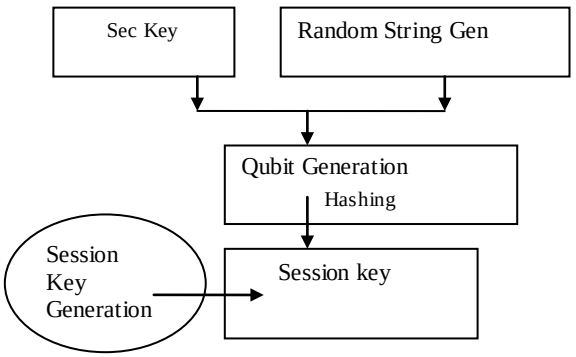

Fig 2:Session key generation

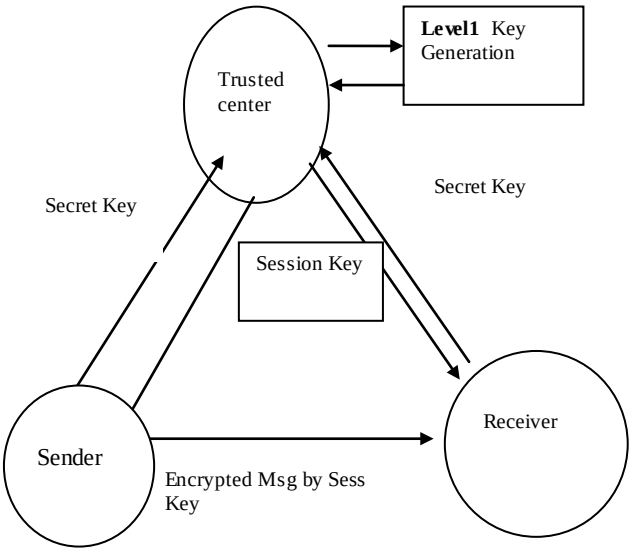

Fig 3:Encrypted key generation

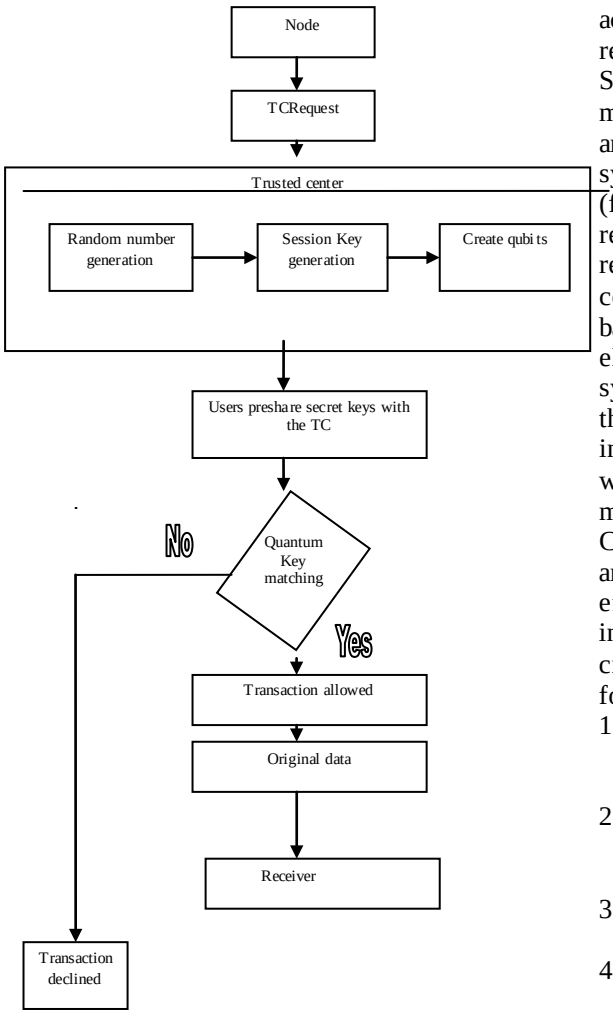

Fig4: Key Matching

IMPLEMENTATION:

Resnick et defines the reputation system as "a system that collects, distributes, and aggregates feedback about consumer's past behavior". The authors outline the problems in eliciting, distributing, and aggregating feedback. Resnick et al. explain the problem of pseudo spoofing in. Pseudo spoofing is the use of multiple pseudonyms in a system by the same real-life entity. The disadvantage is that any entity can discard a handle or a pseudonym with which a bad reputation is associated and join the system as a new user, under a new pseudonym. This can possibly nullify the usefulness of a reputation system, which assigns reputations to handles. The authors also advocate that the newcomers should pay their dues in order to mitigate the effect of pseudo spoofing. In other words, the newcomers should not only use the services of the system but should also contribute to the system as per the system guidelines. Peer Trust allocates the reputation information to a certain node on the network for storage, by using hash functions. Any peer looking for the reputation of another peer uses the search mechanism of the underlying network to search for the information. The authors of Peer Trust argue that trust models based solely on feedback from other peers in the community are ineffective and inaccurate. The authors recommend the "degree of satisfaction" of the peer from previous transactions and the number of transactions a peer performs in the system should be accounted for before calculating the reputation of the recommended peer. Client-Server (Centralized) Reputation Systems In the reputation systems based on the client-server model, the server provides pseudonyms (identities) to users and inducts them into the system. Once logged into the system, a requester (client) selects a service provider (server) (from other users) for a given service, based on the reputation of the service provider. The requester then receives a service from the provider. Once the transaction is complete, the requester gives recommendation to the server based on its satisfaction level from the transaction. Amazon, eBay, and Monster follow the client-server-based reputation system. Although the server forms a single point of failure, the users (clients) trust the server to ensure the security and integrity of the reputation data of users. Some of the other websites, which use various kinds of reputation mechanisms, are moviefinder.com, reel.com, and CDNOW.com. Quantum cryptography easily resists replay and passive attacks, whereas classical cryptography enables efficient key verification and user authentication. By integrating the advantages of both classical and quantum cryptography, this work presents two QKDPs with the following contributions:

1. man-in-the-middle attacks can be prevented, eavesdropping can be detected, and replay attacks can be avoided easily;
2. user authentication and session key verification can be accomplished in one step without public discussions between a sender and receiver;
3. the secret key preshared by a TC and a user can be long term (repeatedly used); and
4. the proposed schemes are first provably secure QKDPs under the random oracle model.

In the proposed QKDPs, the TC and a participant synchronize their polarization bases according to a pre shared secret key. During the session key distribution, the pre shared secret key together with a random string is used to produce another key encryption key to encipher the session key. A recipient will not receive the same polarization qubits even if an identical session key is retransmitted.

Consequently, the secrecy of the pre shared secret key can be preserved and, thus, this preshared secret key can be long term and repeatedly used between the TC and participant. Due to the combined use of classical cryptographic techniques with the quantum channel, a recipient can authenticate user identity, verify the correctness and freshness of the session key, and detect the presence of eavesdroppers. Accordingly, the proposed QKDPs require the fewest communication rounds among existing QKDPs.

The same idea can be extended to the design of other QKDPs with or without a TC. The random oracle model is employed to show the security of the proposed protocols. The theory behind the random oracle model proof indicates that when the adversary breaks the three-party QKDPs, then a simulator can utilize the event to break the underlying atomic primitives. Therefore, when the underlying primitives are secure, then the proposed three-party QKDPs are also secure.

CONCLUSION

Witness transfer from a colluding group of witnesses to an honest one should not lead to propagation of incorrect information. This study proposed two three-party QKDPs to demonstrate the advantages of combining classical cryptography with quantum cryptography. Compared with classical three-party key distribution protocols, the proposed QKDPs easily resist replay and passive attacks in p2p systems. It reduces attacks in reputation in p2p system. Compared with other QKDPs, the proposed schemes efficiently achieve key verification and user authentication and preserve a long term secret key between the TC and each user. Additionally, the proposed QKDPs have fewer communication rounds than other protocols. Although the requirement of the quantum channel can be costly in practice, it may not be costly in the future. Moreover, the proposed QKDPs have been shown secure under the random oracle model. By combining the advantages of classical cryptography with quantum cryptography, this work presents a new direction in designing QKDPs Reputation Models.

ACKNOWLEDGMENT

.I feel elated to extend our floral gratitude to VIGNAN'S INSTITUTE OF INFORMATION TECHNOLGY, DEPARTMENT OF CSE STAFF MEMBERS there encouragement all the way of during analysis of this paper there insinuations and critisms are the key behind the successful completion of the paper.

REFERENCES

[1] NextBus, http://www.nextbus.com/, Jan. 2004.

[2] Google RideFinder Home Page, http://labs.google.com/ ridefinder, Feb. 2006.

[3] H. Garett, "Tragedy of Commons," Science, vol. 162, pp. 1243-1248, 1968.

[3] I. Stoica, R. Morris, D. Liben-Nowell, D. Karger, M.F. Kaashoek, F. Dabek, and H. Balakrishnan, "Chord: A Scalable Peer-to-Peer Lookup Service for Internet Applications," Proc. ACM SIGCOMM, pp. 149-160, Aug. 2002.

[4] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Schenker, "A Scalable Content-Addressable Network," SIGCOMM Computer Comm.. Rev., vol. 31, no. 4, pp. 161-172, 2001.

[5] A. Rowstron and P. Druschel, "Pastry: Scalable, Decentralized Object Location, and Routing for Large-Scale Peer-to-Peer Systems," Proc. IFIP/ACM Int'l Conf. Distributed Systems Platforms (Middleware), pp. 329-350, Nov. 2001.

[6] G. Networks, "Groove Networks," http://www.groove.net/ products/workspace/securitypdf.gtml, 2009.

[7] R.L. Rivest and B. Lampson, "SDSI: A Simple Distributed Security Infrastructure," Proc. Crypto '96, pp. 104-109, Aug. 1996.

[8] N. Li and J.C. Mitchell, "RT: A Role-Based Trust-Management Framework," Proc. Third DARPA Information Survivability Conf. and Exposition (DISCEX III), Apr. 2003.

[9] D. Ferraiolo and R. Kuhn, "Role-Based Access Controls," Proc. 15th Nat'l Computer Security Conf., May 1992.

[10] D. Chaum, "Blind Signatures for Untraceable Payments," Proc. Advances in Cryptology (Crypto '82), 1983.

[11] L. Zhou, F. Schneider, and R. Renesse, "COCA: A Secure Distributed Online Certification Authority," ACM Trans. Computer Systems, vol. 20, no. 4, pp. 329-368, Nov. 2002.

[12] M. Chen and J.P. Singh, "Computing and Using Reputations for Internet ratings," Proc. Third ACM Conf. Electronic Commerce, pp. 154-162, 2001

[13] M. Hauswirth, A. Datta, and K. Aberer, "Handling Identity in Peer-to-Peer Systems," Proc. Sixth Int'l Workshop Mobility in Databases and Distributed Systems, in Conjunction with 14th Int'l Conf. Database and Expert Systems Applications, Sept. 2003.

[14] P. Zimmermann, The Official PGP User's Guide. MIT Press, 1995.

[15] P. Dewan, "Injecting Trust in Peer-to-Peer Systems," technical report, Arizona State Univ., 2002.

[16] A. Clausen, "How Much Does it Cost to Buy a Good Google Pagerank?" unpublished, Oct. 2003.

[17] G. Shafer and J. Pearl, Readings in Uncertain Reasoning. Morgan Kaufmann, 1990.

[18] F.K. Robert and A. Wilson, The MIT Encyclopedia of the Cognitive Sciences (MITECS). Bradford Books, 1999.

[19] D.P. Foster and H.P. Young, "On the Impossibility of Predicting the Behavior of Rational Agents," technical report, John Hopkins Univ., 1999.

[20] Dewan And DASGUPTA: P2P Reputation Management Using distributed identifiers and decentralized recommendation 1013