International Journal of Information, Control and Computer Sciences
ISSN: 2517-9942
Vol:3, No:5, 2009

Secure peerTalk Using PEERT System

Nebu Tom John, and N. Dhinakaran

***Abstract*—**Multiparty voice over IP (MVoIP) systems allows a group of people to freely communicate each other via the internet, which have many applications such as online gaming, teleconferencing, online stock trading etc. Peertalk is a peer to peer multiparty voice over IP system (MVoIP) which is more feasible than existing approaches such as p2p overlay multicast and coupled distributed processing. Since the stream mixing and distribution are done by the peers, it is vulnerable to major security threats like nodes misbehavior, eavesdropping, Sybil attacks, Denial of Service (DoS), call tampering, Man in the Middle attacks etc. To thwart the security threats, a security framework called PEERTS (PEEred Reputed Trustworthy System for peertalk) is implemented so that efficient and secure communication can be carried out between peers.

***Keywords*—**Key management system, peer-to-peer voice streaming, reputed trust management system, voice-over-IP.

I. Introduction

LIVE streaming applications have enormous and ever increasing popularity in real-life deployment. It involves both audio and video applications. The paper peerTalk [1], a peer to peer multiparty voice-over-IP system describes about multiparty voice-over-IP services using application end points, such as peer hosts. The peerTalk services allow a group of people to freely communicate with each other via internet which has many applications as massively multiplayer online gaming [17], telechorus, online stock marketing, etc. It achieves better scalability and failure resilience when compared to existing approaches like P2P overlay multicast and coupled distributed processing services.

The peerTalk [1] presents three unique features. First, peerTalk provides the decoupled distributed processing approach (DDP) for MVoIP session which is shown in Fig. 1. The DDP partitions the multi stream into (a) mixing phase, which mixes audio stream of all active speakers into single stream. (b) distribution phase, which distributes mixed audio stream to all listeners. Second, peerTalk is fully distributed and self-organizing, which does not require any specialized servers. Thus, the peerTalk can naturally scale up as more peers join the system. Third, peerTalk is adaptive, which can dynamically grow or shrink the mixing tree based on the current number of active speakers.

Nebu Tom John is with Department of Information Technology, Karunya University, Tamil Nadu, India doing post graduation in Network and internet engineering (e-mail: sweetcoolnebu@gmail.com).

N. Dhinakaran is with Department of Information Technology, Karunya University, Tamil Nadu, India (e-mail: kndhina@karunya.edu).

The multiparty voice-over-IP (MVoIP) service is vulnerable to various security threats like node misbehavior, Sybil attack, malicious threats, call tampering, eavesdropping , Denial of Service (DoS), Man in the Middle attack etc. Node misbehavior is one of the major threats faced by the MVoIP services. Since some nodes become greedy, they consume resource from other nodes but refuse to share resources. Moreover these nodes refuse to forward the voice packets and results in Denial of Service (DoS). In Sybil attack, the malicious parties can compromise the network by generating and controlling large numbers of shadow identities. The attacker can tamper the call for accessing private informations.

In this paper a security framework called PEERTS (**PEE**red **R**eputed **T**rustworthy **S**ystem for peertalk) is proposed for the peerTalk so that authentication, authorization, confidentiality and integrity can be achieved. It involves reputation-based, distributed trust architecture for the peerTalk network to identify attacking peers and to prevent the spreading of malicious content. The key management system [13] is also introduced to secure the peerTalk session.

Reputation-based trust management [12] systems are used to establish trust among members of on-line communities where parties with no prior knowledge of each other use the feedback from their peers to assess the trustworthiness of the peers in the community. One well-known such system is the rating scheme used by the eBay on-line auction site [11].

The rest of the paper is organized as follows: section II discusses the security threats affecting peerTalk. Section III introduces new framework called PEERTS security framework. The performance analysis is presented in section V. Section VI discusses related work. In the last section, we present conclusion.

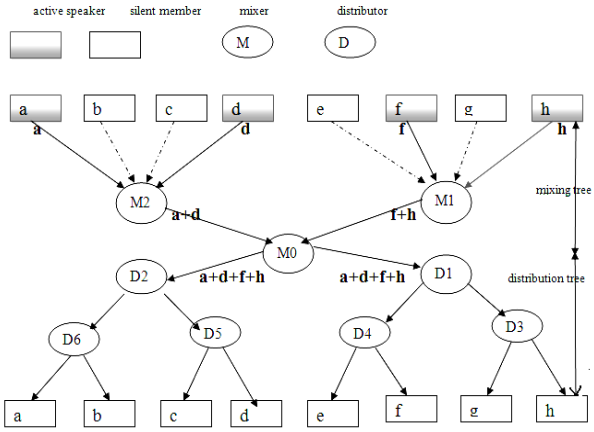

Fig. 1 Decouple service model used in peerTalk [1]

II. Security Threats Affecting PeerTalk

In this section, the major threats affecting the peerTalk: A peer-to-peer multiparty voice-over-IP (MVoIP) system is discussed. It involves nodes misbehavior, Sybil attack, eavesdropping, Denial of service (DOS), call tampering, man in the middle attack.

A. Node Misbehavior

This is one of the major threats in peerTalk [4]. Peer to peer network rely on the cooperation of all participation nodes. The cooperation requires detecting routes and forwarding voice packets. However, it consumes network-bandwidth, local CPU time, memory and energy. Therefore there is a strong motivation for a node to deny packets forwarding to others and being selfish. Even if some nodes have more resource and have less delay between source and all other participants and refuse to become the root mixer. More over some nodes will also deny becoming the intermediate mixer.

The peerTalk decouples the MVoIP service delivery into two phases like mixing phase and distribution phase. For the mixing process, the service provisioning protocol is used to find the root mixer. Each peer run DVMRP algorithm [1] to construct multicast trees routed at themselves. Each peer measures average delay of its own multicast tree and then propagates the delay information plus its mixing capacity to all others members via the overlay mesh. All peers then select the same as root mixer. Maybe some peer will become greedy and refuse to send correct delay and capacity information to other peers and thus misbehaves. This misbehavior will happen for both root and non root mixing and merging. The proposed approach to overcome nodes misbehavior is to use the reputation based trust management.

B. Sybil Attack

Sybil attack [5], [6] is another threat in the peer to peer system. In Sybil attack, a single faulty entity can present multiple identities so that it can control a substantial fraction of the system. The attacker can pretend multiple identities and thus consumes the resource of the root mixer and thus results in the denial of service

Sybil attack also affects online gaming applications. In online games, the Sybil attack may happen when the malicious user pretends multiple identies and makes him to win the particular game. The malicious user can control that particular network. One approach to prevent these Sybil attacks is to have trusted agency certify identities.

C. Eavesdropping and Traffic Analysis

Eavesdropping [2], [3] is another security threat affected by the peertalk. This is the way in which the hackers steal credential and other information. Through eavesdropping, the third party can obtain names, passwords and phone numbers, allowing them to gain control over voice mail, calling plan, call forwarding and billing information. This leads to service theft. This is mainly done by the monitoring of the traffic carried out between the genuine speakers. The eavesdropping can be avoided by the use of the keymanagement. The voice packet should be encrypted inorder to attain the confidentiality. The challenge with voice is to encrypt strongly and quickly, to protect confidentiality and as not to slow down the packet flow.

D. Call Tampering

Call tampering [18] is an attack which involves tampering a phone call in progress. The attacker can simply spoil the quality of the call by injecting noise packets in the communication stream. He can also withhold the delivery of packets so that communication become spotty and the participants encounter long periods of silence during the call.

E. Denial of Service (DoS)

Denial of service [7], [8], [9] may happen by making computer resource or network bandwidth unavailable for legitimate users. The attacker consumes the network bandwidth of the root mixer and non root mixer. As the consumption increases, the usage of the non root splitting and merging increases and results in the denial of service. .

DoS attacks can be carried out by flooding a target with unnecessary SIP call- signaling messages, thereby degrading the service. This causes calls to drop prematurely and halts call processing. Once the target is denied of services and ceases operating, the attacker can get remote control of the administrative facilities of the system. DoS attacks can be overcome by the reputation based trust management.

F. Man in the Middle attack

This attack is also known as spoofing [10]. Spoofing requires hacking into a network and intercepting packets being sent between two parties. Once the IP address or phone number of the host is discovered, hackers can use this attack to misdirect communications, modify data and transfer cash from a stolen credit card number. This attack can be avoided by employing encryption technique.

III. PEERTS Security Framework

PEERTS (PEEred **R**eputed **T**rustworthy **S**ystem for peerTalk) is the security frame work created for the peerTalk. It consists of distributed reputed trustworthy system to establish trust among the peers to create a secure peer to peer multiparty VoIP system. The fully distributed reputed trust management system is based on modified Bayesian network-base trust model. Key management schemes are also introduced in PEERTS. Since the peertalk has important applications such as online gaming, teleconferencing, online stock trading, telechorus, etc. the PEERTS play an important role. Without the PEERTS security framework, the multiparty VoIP systems are vulnerable to various attacks and will be insecure to the users.

PEERTS security frame work consists of the following components as shown in the Fig. 2: **The Monitor**, **the Reputation based Trust Management System, the Key Manager.** The components are present in every node.

A. The Monitor

In peer to peer networking environment, the nodes used to lookup every other peer. The monitoring process is to detect the unusual behavior such as intrusion, nodes misbehavior, denial of service (DoS), etc.

For peerTalk, each peer sends heartbeat messages to its neighbors to indicate its liveness and stream processing. Each peer can keep the up-to-date neighbor list and neighbor information based on the heart beat messages. Each peer also periodically monitors the network delay to its neighbors and bandwidth of the corresponding links using active probing. Each peer maintains the routing costs (network delay) to every other peer and the path that lead to such a cost [1]. While updating neighbor list, the node compares with the previous list. It involves the comparison of the previous routing costs with the current. If the deviation is monitored, then it will call the reputed trust management system to check whether that node misbehaves or not.

B. The Reputed Trust Management System

The fully distributed reputation based trust management system is [14], [15] based on a modified Bayesian estimation procedure. It is used to establish trust among members of on-line gaming communities or teleconferencing or online stock trading applications were parties with no prior knowledge of each other use the feedback from their peers to assess the trustworthiness of the peers in the community.

The proposed reputation based distributed trust architecture for the peerTalk is to identify malicious peers and to prevent the spreading of malicious content. Each peer maintains the routing costs of the neighbor nodes (network delay and bandwidth). Periodically nodes update the routing costs of the neighbor nodes. So the comparison occurs with the previous routing costs and the current routing costs and thus the behavioral value is calculated.

Each node maintains the trust rating such that if the behavioral rating goes beyond the threshold trust rating, then there is evidence of malicious behavior. And if the behavioral rating is less than the trust rating, the nodes still are good behavior.

- Behavioral value = comparison of previous routing costs and current routing costs.
- Misbehavior Node = Behavioral value goes beyond threshold trust rating
- Good behavior Node = Behavioral value less than threshold trust rating.

Once the reputed trust management system found the misbehaved neighbor node, it will undergo the action as the deletion of paths containing malicious nodes or either ignoring the request from the malicious nodes. After the selection of the good behavior nodes, the key management functions.

When a peer wants to join an existing MVoIP session, it is first incorporated into the P2P overlay mesh by an out-of-band bootstrap mechanism [16]. The peer selects a few peer hosts provided by the bootstrap service as neighbors and also requests a few other peers to add itself as a neighbor. After the peer successfully joins the overlay mesh, it can request the other peer to join the session. The peer can acquire the session ID from the bootstrap service done by key management after reputed trust management evaluation occurs.

C. The Key Manager

The key manager [13] is used to provide the session ID to all the participating nodes. After the trustworthy calculation is made, the participating good behavior nodes will be given session key by the selected rendezvous point that serves as the root of both mixing tree and mixing tree. The participating nodes will send their public keys to the root mixer and the root mixer will send encrypted session keys to all participating nodes. The participating nodes will decrypt the session keys by using their private keys. The communications should be carried out by using encrypted session keys.

After the particular period, the session keys are changed. By using the key management, the eavesdropping, call tampering, man in the middle attack, etc.

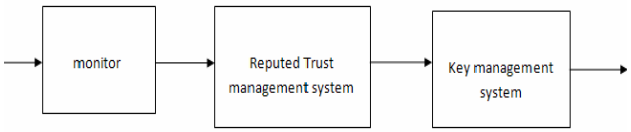

Fig. 2 PEERTS security framework in each node

D. Brief Description of PEERTS

PEERTS is the security framework used in the peerTalk: a peer to peer multiparty voice over IP system. PeerTalk allows a group of people to freely communicate with each other via the internet, which have many applications like online gaming, teleconferencing, online stock trading etc. Compared with the traditional multiparty voice over IP technologies like overlay multicast, coupled distributed processing, server-based centralized audio mixing, PeerTalk achieves better scalability and failure resilience by dynamically distributing the stream processing workload among different peers. Particularly PeerTalk decouples the MVoIP service delivery into two phases: mixing phase and distribution phase. The paper PeerTalk: A peer to peer multiparty voice-over-IP system [1] describes that peerTalk can outperform and will play major role in human life. PeerTalk provide more flexible MVoIP services that allow any participant to speak at any time.

Moreover peerTalk is vulnerable to various attacks since it is processed by the peers. So security framework plays an important role for peerTalk because without that whole system will get crash.

PEERTS security frame work describes that at the beginning of the session, the reputed trust management system calculate the behavioral value of each node. Each peer sends heartbeat messages to its neighbors to indicate its liveness and the current stream processing performance. The peers periodically monitor the network delay and bandwidth of the links (routing costs). While updating the reputes trust management systems compares with previous routing costs and calculate behavior value. If the behavioral value is beyond the threshold trust rating, then the peer is considered as misbehavior node otherwise not.

After all trusted participants run the election protocol to select the rendezvous point that serves as the root of both mixing and distribution tree. Each peer runs the multicast trees and measure minimum average delay of its own multicast trees. And then propagates the delay information plus its mixing capacity to all other members via overlay mesh. All peers then select the same best peer as rendezvous point.

After selecting the rendezvous point, all the other participating peers sent their encrypted public key from their key pairs to the root mixer. The root mixer will decrypt public keys create the session keys and send securely to all peers participating in MVoIP session. Thus each participant will encrypt the voice messages with session key.

The mixer splitting, mixer merging replication process and failure resilience management will happen through the PEERTS security frame work.

If the other participating nodes found that root mixer is misbehaving, then the participating session will be terminated and again the election is carried out for the selection of rendezvous root mixer after the evaluation of the trustworthy.

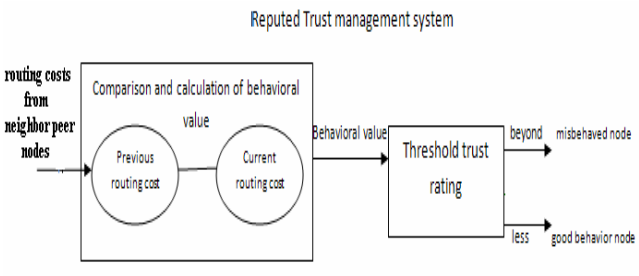

Fig. 3 Structure of Reputed Trust management system

IV. Performance Analysis

We evaluate the performance of the PEERTS (PEEred Reputed Trustworthy System for peerTalk) using network simulator. The objective of the performance analysis is to prove the importance of the PEERTS in peerTalk system. The analysis is carried out in the following metrics

A. Detection Time of the Misbehaving Node

The detection time is measured as the simulation time taken for all misbehaving nodes to be classified as detected by all normal nodes. Fig. 4 shows the detection time of the misbehaving nodes with PEERTS and without PEERTS. Since peertalk with PEERTS uses the second hand information to calculate the behavior value. But the peertalk without PEERTS won't calculate the behavior value. Consider the network of 30 nodes. The weight of behavior value is considered as 0.1 and 0, for the node without considering the behavior value (Fig .4).

B. Overhead

Overhead can be classified as the extra messages required by the PEERTS to attain the reputation which is shown in Fig 4. The overhead used in our reputation system can be measured as the

$O = \sum$ monitoring message sent to reputation system / ($\sum$ request first update + $\sum$ request of second update) (1)

The ratio is plotted (Fig. 5) as overhead ratio with fraction of misbehavior node with pause time.

C. Dropped Packets Due to Misbehaved Nodes

This is the metric used to calculate the efficiency of the peertalk system with PEERTS or not. Packets loss can occur due to link failures, unreachable nodes. It can be calculated as

D = (packets received by root mixer from speakers of the peertalk session) / (packets send by speakers which needed to involve peertalk session) (2)

The dropped packets without PEERTS are high when compared with the PEERTS (Fig.6).

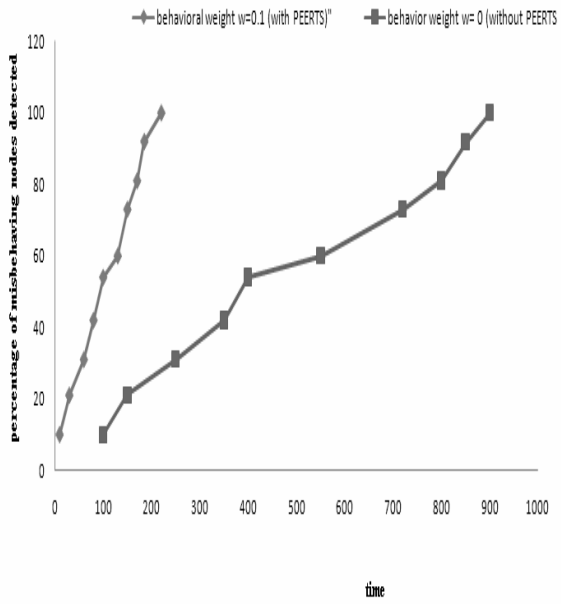

Fig. 4 Mean detection time of all misbehaving node

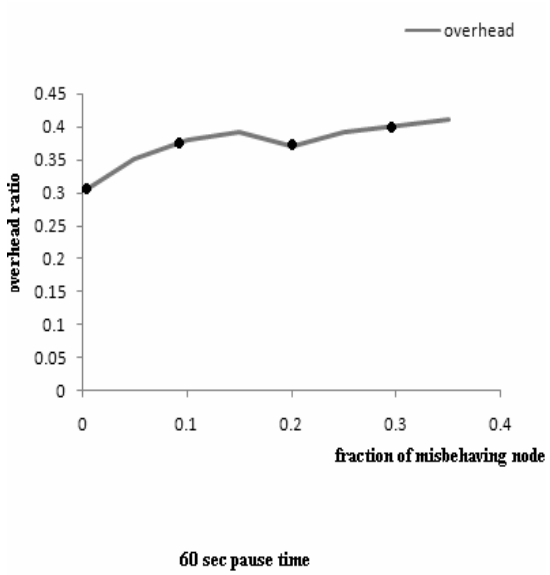

Fig. 5 Overhead plotted against fraction of seconds at 60 sec pause time

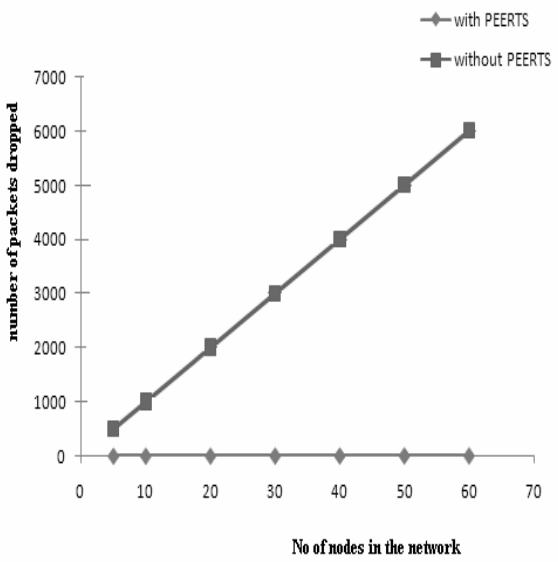

Fig. 6 Mean number of packets dropped

V. Related Works

The peerTalk has many applications in day to day life. It can be used mainly in VoIP system and peer to peer systems. Future works involves the improving the efficiency of the peerTalk with increased security. More over secure peer to peer file sharing using peertalk is under research.

VI. Conclusion

PeerTalk: A peer to peer multiparty voice-over-IP system creates new era in the MVoIP services. The peerTalk achieve better scalability and cost effectiveness by adaptively and efficiently distributing the stream processing workload among the peers. PeerTalk have many applications such as online gaming, teleconferencing, online stock trading etc. But this is vulnerable to various attacks such as nodes misbehavior, denial of service, call tampering, man in the middle attacks, eavesdropping, etc. So a security frame work is needed for the peertalk. The PEERTS is the security framework, the peered reputed trustworthy system for peertalk. The reputed trustworthy system is used to rate the nodes take part in the peertalk session. Key management is also introduced in this framework. The PEERTS shows that detection of the misbehaved node is very high and also reduces the dropped packet due to misbehaved node and thus efficient. The efficiency and the capability of the peerTalk are increased by introducing the PEERTS security framework.

References

[1] Xiaohui Gu, Zhen Wen, Philip S.Yu, Zon-Yin Shae , PeerTalk: A peer-to-peer multiparty Voice-over-IP System. IEEE transactions on parallel and distributed systems , April 2008
[2] Vulnerabilities and Security Threats in Structured Peer-to-Peer Systems: A Quantitative Analysis.Madhukar srivastava and Ling Liu .
[3] Sufficiently secure peer- to-peer networks. Ruper Gatti, Stephen Lewis, Andy ozment,Thierry Raynal, Andrei Serjantov.
[4] A Node Misbehaviour Detection Mechanism for Mobile Ad-hoc Networks, Tarag Fahad & Robert Askwith.
[5] A survey of solutions to the Sybil attack. Brian Neil, Levine Clay Shields, N. Boris Margolin.
[6] Defending the sybila attack in P2P network: Taxonamy, challenges and a proposal for self registrtation. Jochen Dinger, and Hannes Hartenstein. Instite f'ur Telematik,Universit" at Karlsruhe (TH, Germany dinger@tm.uka.de, Hartenstein@rz.uni-karlsruhe.de.
[7] Method and system for overcoming Denail of service attacks. Mark Vange, Mark Plumb, Kevin Blumberg.
[8] Preventing DoS attacks in peer to peer media streaming systems. William Connor, klara Nahrstedt, Indranil Gupta Department of computer science, university of Illinois, Urbana,IL USA.
[9] System and method for addressing Denial of Service attacks. Bruce wallman.
[10] Man in the middle attack on the authentication of the user from the remote autonomous object, Cheng-Ying Yang, Cheng Chi Lee and Shu – Yin Hsiao4.
[11] EBay. http://www.ebay.com.
[12] P. Resnickand, R. Zeckhauserand, E. Friedman, and K. Kuwabara. Reputation systems. Communications of the ACM, 43(12), 2000.
[13] Secured Peer to Peer network data exchange. Kuldip singh pabla, santa clara (US); William j.Yeager. Menlo Park, CA (US).
[14] A Reputation-Based Trust Management System for P2P Networks, Ali Aydın Selçuk Ersin Uzun Mark Res¸at Pariente Department of Computer Engineering Bilkent University,Ankara, 06800, Turkey.
[15] Trust and Reputation in peer-to-peer networks, a dissertation, submitted to the department of computer science and the committee on graduate studies of stanford university, in partial fulfillment of the requirements for the degree of doctor of philosophy.
[16] Y.-H. Chu, S. G. Rao, S. Seshan, and H. Zhang. Enabling Conferencing Applications on the Internet using an Overlay Multicast Architecture. Proc. of ACM SIGCOMM, San Diego, CA, August 2001.
[17] A. Bharambe, V. Padmanabhan, and S. Seshan. Supporting Spectators in Online Multiplayer Games. Proc. of HOTNETSIII, San Diego, November 2004.
[18] http://voip.about.com/od/security/a/SecuThreats.htm