International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 5989-6001
© Research India Publications
http://www.ripublication.com

Reputation System for Improving Security in Voice over Internet Protocol

[1]Mr.Jayaprakash

Department of Computer Applications
Vidyaa Vikas College of Engineering and Technology, Tiruchengode
prakash_zones@yahoo.com

[2]Dr.A.Tamilarasi

H.O.D / Department of Computer Applications
Kongu Engineering College, Perundurai
angamuthu_tamilarasi@yahoo.com

[3]Dr.P.Sriramya

Department of Computer Science and Engineering
Saveetha School of Engineering, Chennai
sriramya82@gmail.com

Abstract

Voice over Internet Protocol (VoIP) is built based upon the communication of a number of application protocols on the Internet. The open architecture of the Internet makes VoIP protocols focuses to more attacks. Spammers be set to to create an atmosphere of untrust in the granted services along with the tools used for the provision. Spam appears as an original threat to the service providers and strives to conflict using in particular some filtering procedures. These filters are not always well-organized as they have to make sure before removing any message that the latter is a spam message with an extremely high assurance. Also these filters should be monitored and well-run regularly. Reputation systems are mechanisms used in various unlike areas to build trust among members of a certain community. The Session Initiation Protocol (SIP) and the Real Time Transport Protocol (RTP) are the leading VoIP signaling protocol and media transport protocol. This work projected a novel trust and reputations based on inter domain connections to improve the security of VoIP using Session Initiation Protocol (SIP). Trust management helps to improve the security of VOIP.

Keywords: Voice over Internet Protocol (VoIP), SPam over Internet Telephony (SPIT), Session Initiation Protocol (SIP), Trust and reputation.

1. INTRODUCTION

Voice communication passed out using the Internet Protocol (IP) for the transportation is known as Voice over Internet Protocol (VoIP). Traditional phone networks which is called as Public Switched Telephone Networks (PSTN) uses circuit-switching [1]. In *Circuit-Switching*, resources and components are well reserved along with the entire communication channel for the period of the call. Equally, Internet Protocol (IP) uses the packet-switching. In *Packet-Switching*, information is digitally transmitted as one or more number of packets. Packets know their destination, and they may arrive their destination through different paths.

Implementing VoIP requires a wide range of protocols in which it requires call signaling for establishing the call and also, to transport real-time voice from corner to corner in the network, to do (QOS) quality-of-service-aware routing, resource reservation, QoS-aware network management and also billing. VoIP network has become widely deployed. They also provide several advantages mostly sufficient in traditional telephony and it become actually appealing to the service providers and expected end users [2].

As there is no dedicated network is used for VoIP, the user may be exposed to unusual attacks like Denial of Service (DoS), Eavesdropping, Hijacking, etc. VoIP technology is being proved with more mature due to its improved functionality, many VoIP devices and services can provide security threats if it is not properly configured. VoIP protocol suite is commonly divided into two categories, control plane protocols and data plane protocols. The control plane portion in VoIP protocol is used for traffic necessary to connect and to maintain the actual user traffic.

It is main responsible for maintaining overall network operation (router to router communications). The data plane (voice) portion of the VoIP protocol is to monitor the actual traffic that needs to get from one node to the node [3]. VoIP utilizes IP for its basic transport method. VoIP utilizes two protocols such as the Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) over IP. The next figure shows the protocol stack for a VoIP network. It is most essential to note that VoIP works with any protocol stack that also supports IP.

End users of VoIP can affix enterprise VoIP systems to their already existing infrastructure relatively rapidly and easily. VOIP systems can obtain a wide variety of forms, along with the traditional telephone handsets, conferencing units, and mobile units. Along with the end-user equipment, VOIP systems consists of a variety of other components, together with call processors/call managers, gateways, routers, firewalls, and protocols. Nearly, maximum of these components have counterparts that is used in data networks, but the performance burden of VOIP mean that ordinary network software and hardware must be enhance with special VOIP components.

Quality of Service (QoS) is primary to the operation of a VOIP network that meets users' quality potential. The implementation of various security measures may also cause a marked deterioration in QoS [4]. These mentioned complications vary from firewalls delaying or blocking call setups to encryption-produced latency and delay variation (jitter). Because of the time-critical nature of VOIP, and its low tolerance for disruption and packet loss, most security measures implemented in various data networks are simply not related to VOIP in their recent form; firewalls, intrusion detection systems, and other components must be specific for VOIP.

The Session Initiation Protocol (SIP) is an application-layer signaling-control protocol that is used to establish, maintain, and terminate multimedia sessions. Multimedia sessions comprise VOIP, conferences and other related applications linking such media as audio, video and data. SIP, on which the RFC 2543 is based, is a text-based protocol which is a piece of the overall Internet Engineering Task Force (IETF) multimedia architecture.

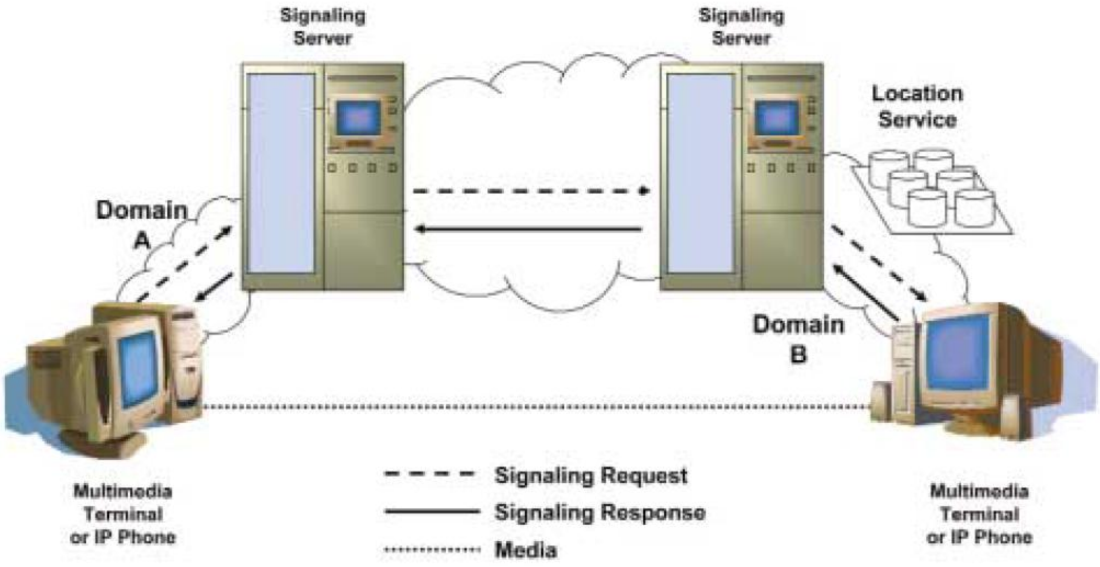

Figure 1 Simple VoIP Configuration

The IETF architecture also contain the Resource Reservation Protocol (RSVP; RFC 2205), Real-Time Transport Protocol (RTTP; RFC1889), and Session Description Protocol (SDP; RFC 2327). The SIP's functions are mainly independent of some functions of these specified protocols [5]. It is very significant to mark that SIP can activate in conjunction with extra signaling protocols, such as H.323.

In SIP, authentication and authorization are being handled as "*either on a request-by-request basis along with a challenge/response mechanism, or also by using a lower layer scheme*". Since SIP is a very lightweight protocol, their security facilities are very limited [6]. SIP requests and responses cannot be made end-to-end encrypted because of the message fields such as the request and route must to be able to be seen to proxy servers that are here in many network architectures to make sure

SIP requests are routed appropriately. Voice data is transmitted in clear text over UDP and TCP.

As VoIP usage increasing widely, so will the pesky marketing strategies linked with it. Perennial annoyances similar to telemarketing and spam have been plaguing consumers and internet users used for years. A new sort of hybrid mixture of these two concepts is SPIT, or spam over internet telephony. Similar to email spamming, sending commercial messages via VoIP is very fast and also cheaper. Nothing like traditional telemarketing, although, VoIP provides the potential for huge volumes of unsolicited calls, suitable to the wide array of tools previously existing to attackers on the internet. Telemarketers with no trouble can send large amounts of messages to VoIP customers.

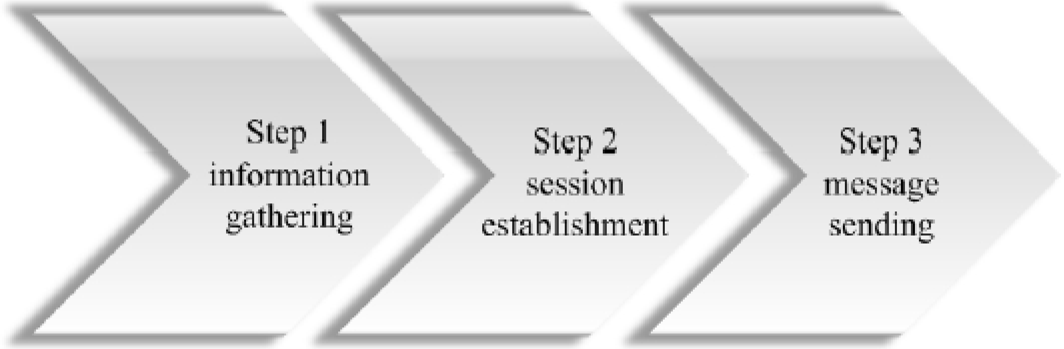

Figure 2 Three steps of SPIT

Nothing like traditional spam email messages, which are average only 10–20 kilobytes in file size, unnecessary VoIP voicemails can involve megabytes of storage. The acceptance of VoIP technologies and services by end-users is robustly depended and strongly connected to the avoidance of Spam over Internet Telephony (SPIT). In IP telephony SPIT typically refers to unsolicited bulk calls. However, in addition to this fundamental form of SPIT, three different forms are well-known [7, 8]:

1. Call SPIT, is defined as a mass unsolicited set of session initiation attempt to facilitate launch a multimedia session.
2. Instant Message SPIT, is defined as a mass unsolicited set of immediate messages, and is much related to email spam messages.
3. Presence SPIT is defined as a mass unsolicited set of existence requests for the initiator of SPIT to develop into a part of the address book of a user or potentially of multiples users.

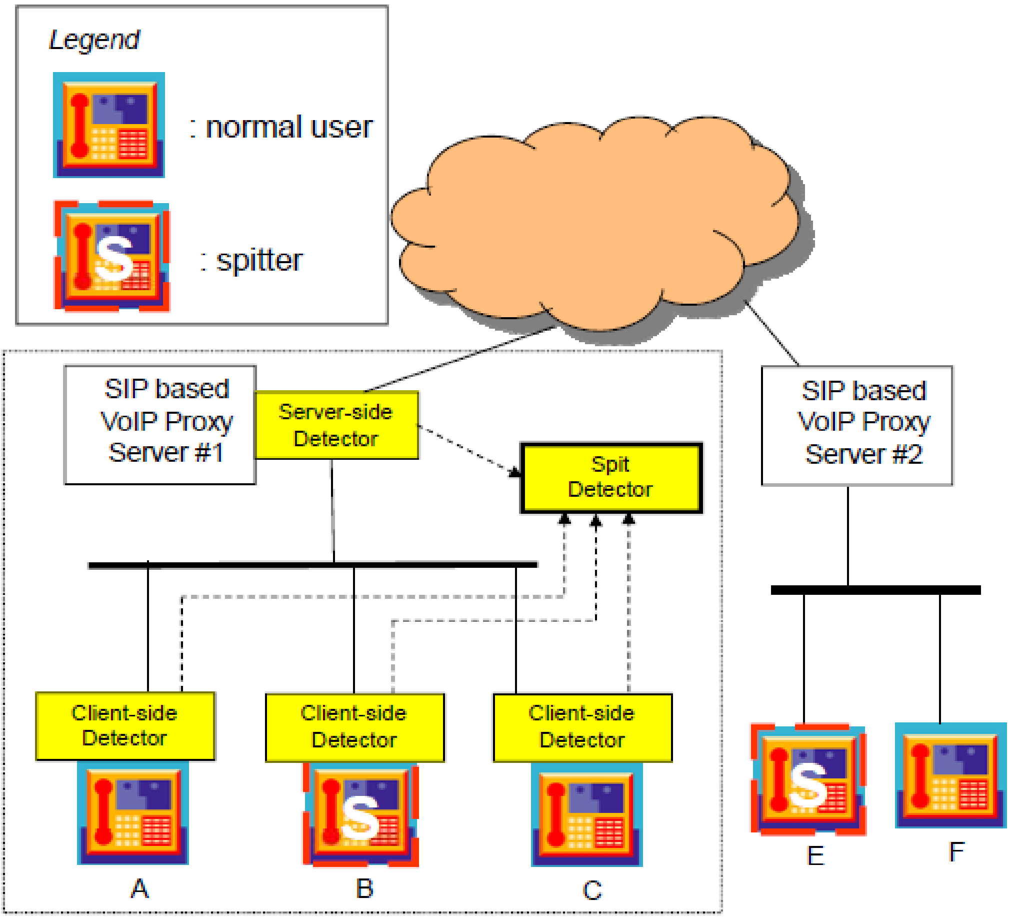

Figure 3 Detecting Spit Calls in a VoIP Environment

A blacklist-based method can be used to establish call phase based on source IP or from URI to drop calls from well-known SPIT source. In the media stream phase, a representative pattern one can imagine for SPIT calls is the caller speaks more than the callee. Another pattern is the extent of the media stream phase which is the call duration, and it is very shorter if in the case of calls answered by a live person as SPIT calls are in general undesirable [9]. Moreover, one can think that it is more expected that for a SPIT call, a call termination will be begin by the callee i.e., the callee launch the SIP BYE message.

In this above work we offer a novel trust and reputation based inter domain connections for mainly improving the security of VOIP with SIP protocol. Trust management can assist civilizing the security of VOIP. For recognizing the spam point a client may require to trust other clients in its domain for examination anomalous measurements. Reputation of trust in VOIP contains data disclosure decisions and also key exchange. Section 2 assesses the linked work in literature. Section 3 clarifies the methodology. Section 4 talks about the results and Section 5 brings to a close the work.

2. RELATED WORK

Lentzen et al., [10] calculated a robust audio fingerprint of spectral feature vectors that is for incoming audio data. Along with a database of feature vectors, new calls were matched up to with previous ones and replays with identical or similar audio data are identified. Based on the strategy, future calls starting the same source can next be blocked for the duration of call setup. A prototype based on this particular approach can develop and first results demonstrated the system can efficiently detect and block Spam calls.

Khan et al., [11] talked about the difficulty of spam over IP telephony and examined techniques which make use of the SIP to reject expected nuisance callers. Existing techniques integrated content filtering, black lists, white lists, gray lists, call rate monitoring, IP/domain correlation, consent-based connections, reputation system, address obfuscation, limited-use addresses, computational riddle, payments on risk, legislation, circles of trust, centralized SIP providers, and authenticated identity. A inventive method on using a text-based Turing test was projected and confirmed to be compatible with the SIP protocol.

Chang et al., [12] inspected the use of TCG remote attestation method to get enhanced the security of SRTP/ZRTP channel equipment. The security belongings were comprehensive which a belief channel method should have. Then a trusted SRTP/ZRTP channel procedure was projected and related model checker SPIN to validate that the proposed method could achieve the declared security properties.

Falk et al., [13] expressed the method identity cards can be included in SIP-based voice over IP telephony to constantly recognize users and authenticate participants using as example the German “Elektronischer Personalausweis” (ePA). Though, providing trusted identities in a realistic way is still a not easy problem. Identity cards have been initiated by several countries supporting electronic authentication and identification of citizens, e.g., the German ePA. As many German citizens will possess an ePA soon, it can be used as security token to endow with trusted identities. Authentication and identification are most important building blocks in the safety measures of VoIP communication, keying material launched during authentication can be used for additional protection of the communication.

Lin et al., [14] projected a trust degree-based dynamic model for protecting the VoIP above WMNs, in which every node preserves trust degree for further nodes and practical the trust degree to assess the trustworthiness. The performance of the projected form was confirmed with simulation outcome.

Thanthry et al., [15] projected an interchange encryption system that uses PKI architecture for the first authentication and key exchange, and encrypted the real-time traffic with a symmetric algorithm using a exclusive key for each and every packet. The proposed algorithm probable to be less complex matched up to the traditional encryption schemes along with enhancing the security of the communication. Initial analysis hold out by the authors pointed out that the planned scheme assisted in improving the voice quality to a definite extent as sustaining the security of the communication.

Deng & Shore [16] inspected to prove how denial of service attacks changes the performance of a SIP-based system, and projected an Improved Security-

Enhanced SIP System (ISESS) to mitigate such type of attacks. Experimental results were offered to exhibit the efficiency of ISESS. The investigational results demonstrated that with ISESS, during a flood-based denial of service attack, the performance of the system can be improved significantly.

Pelaez [17] talk about a methodical approach to assess steganography in VoIP uses misuse patterns. Misuse patterns explained from the attacker view, explained how a kind of information misuse was executed, examined the ways of discontinuing the attack, and measured how to sketch the attack happened. The pattern tries to associate events with definite division of the system. The semiformal models are used as a technique to advance the discovery of embedded secreted messages in IP telephony.

Azad & Morla [18] projected a social strength for sensing SPIT callers. Authors examined how likeness and social binds among VoIP users result SPIT detection. A different characteristic of the projected approach explains that no involvement of users for comment and it can be simply organize in real VoIP network with no a few change in structural design and SIP protocol stack. The social strength move toward was assess on dissimilar kinds of random network data and demonstrated that the system senses SPIT callers with false positive rate still less than to 10% and true positive rate with 99% inclusive for all the type of primary random networks.

Yu [19] wished-for P2PSIP (Peer-to-Peer SIP) to offer fully dispersed multimedia communication arrangement. In P2PSIP networks, the address deciding method of the Distributed Hash Table (DHT) superimpose was used to determine the IP address of the matching target user. To get better the query performance of P2PSIP networks, three approaches were planned together with Bidirectional Chord, Asynchronous processing and Load balancing. By evaluating investigational outcome in terms of Registrations-Per-Second (RPS), Calls-Per-Second (CPS) and CSD below usual and better P2PSIP networks, completed that the grouping of these three move toward approaches can efficiently get better the query performance of P2PSIP networks.

Sattar et al., [20] planned a VoIP transmission algorithm to decrease transmission delay in order to add to (QOS) quality of service of VoIP. The authors' intended to utilize IP protocols and offered a method to get better VoIP performance.

Liu [21] applied a formal method, Coloured Petri Nets, to discover and analyze the vulnerabilities of SIP to DoS attacks. Using the approach effectively identified the vulnerabilities with SIP call setup process, which may be exploited to launch DoS attacks on SIP-based VoIP systems. The authors also discussed the possible solutions to the identified security issues.

3. METHODOLOGY

There is presently no method for a getting provider to assess the reliability or the semantics of SPIT-related information acknowledged. The proposed method attempts this crisis by applying a provider-level reputation method, based on the SPIT tags allotted to leaving SIP messages by the caller's provider. The method provides an incentive to attach a label to leaving calls suitably, and it decodes tags with arbitrary semantics into significant SPIT chances. A modular representation that combines trust and reputation: *interaction trust* (results from past knowledge from direct communications) and *certified reputation* is urbanized.

3.1 Interaction trust

Interactions trust (IT) represents the trust that results from the direct communications linking two agents. A commercial transaction was reflected on where agent *a* gets an exacting product from agent *b*. The ending conclusion of the transaction deal possibly will consist of the product's price, quality, and their delivery date. Since this result, agent *a* might provide ratings concerning agent *b*'s service for price, quality, and delivery for those exacting communication. Ratings are thus tuples in the following form: *r = (a, b, i, c, v);* where *a* and *b* are the agents with the intention of contributed in the communication *i*, and *v* is the score rating *a* gave *b* for the expression *c* (e.g. price, quality, delivery). It is given that the range of *v* value is [-1, +1], and if -1 means completely negative, +1 means totally positive, and 0 means neutral or uncertain. If we need to calculate IT from past knowledge, an agent wants to monitor the entire record its past ratings into a (local) *rating database*. While computing the IT value for agent *b* regarding term *c*, agent *a* has to question its database for all the ratings that have the form method (*a, b,_, c,_*), where as the '_' symbol be able to be substituted by any value. We call the set of those ratings *ℛ (a, b, c).* Here the IT is indicated by T_I .It is evaluated out of all the ratings in the set as the weighted mean of the rating values:

$$T_I \ \ a,b,c \ = \sum_{r_i \in R(a,b,c)} \omega(r_i).v_i$$

Whereas v_i is the value of the rating r_i and $\omega(r_i)$ is the weight equivalent to r_i. The weight (r_i) for each rating is chosen so that it gives extra weight to extra recent ratings, with a restriction that

$$\sum\nolimits_{r_i \in R(a,b,c)} \omega(r_i) = 1\,.$$

This is to make sure that the trust value T_I (*a; b; c*) is in the range [-1, +1].

3.2 Certified reputation

Certified reputation (CR) is ratings obtainable by the rated agent (agent *b*) regarding itself which is gained from its partners in past interactions. These ratings are certifications which are provided by the rating agents. These ratings of agent *b*'s past performance are fairly similar to a reference when be relevant for a job). They allow an agent to confirm its attainable performance as observed by preceding interaction partners. As agent *b* can choose the ratings it lays advance, a rational agent will only nearby its best ratings. Therefore, we must imagine the CR information perhaps overvalue an agent's predictable performance. Thus, even though it cannot assure agent *b*'s performance in upcoming communications, the CR information does expose a part viewpoint on agent *b*'s past performance. The major advantage of this kind of information is its very high accessibility. Along with the collaboration of its partners, agent *b* can include CR information from just a tiny figure of communications. so, CR is offered to agents in the majority situation; even in state of affairs where the additional components might fail to offer a trust evaluate. The process of CR is given below [22]:

1. Later than in each and every transaction, *b* requests over its partners to offer their ratings regarding its performance in which it keeps in its databases.
2. When *a* associates *b* to say its importance in using *b*'s examine it ask over *b* to offer reference regarding its history performance.
3. Agent *a accepts* the marks of *b* from *b*. It evaluates the marks' consistency and analyzes a trust value for *b*. Particularly, the value of CR, $T_C(a, b, c)$, and its consistency, $\rho T_C\ (a, b, c)$, are intended as per the WR component, but the input is the set of ratings supplied by the target agent *b* itself.

Reputation method is planned on the level of SIP service suppliers rather than entity users. This is not only for scalability basis or due to a predictable durability of character, but also because we want to make use of the service providers' capability to examine their customers' performance. SSPs have unusual kinds of expectation relationships. Peering concords represent trust that fees will be rewarded. Trust in SSPs' call cataloging competence is recognized, characterized by SPIT probabilities for tupelos as rated units. Each SSP trusts a small set of other providers to correctly report these SPIT probabilities. This small set is what we refer to as "convictional suppliers". A tiny number of dependence suppliers create it easy to treaty with deceptive news, for example with official means, based on bond relationships. This prospect makes it unappealing for any provider to give counterfeit comment about SPIT likelihoods. Therefore, it is realistic not to unambiguously consider the likelihood of a hit by a faithful provider. T (x) will signify the set of a supplier x's convictional providers and one level of transitive trust3 is worked out as

$$U\ x = \bigcup_{y \in T\ x} T\ y \cup T\ x$$

Where U(x) be the set of all supplier trusted by x, either openly or furtively (i.e. together with those hoped by x's in a straight line of trusted suppliers).

4. EXPERIMENTAL RESULTS

Experiments were performed by contrasting the number of calls. The spammers within the calls were diverse from 5% to 15% of spammers. The false positive and false negative is calculated. A false positive is an error where a spam is not identified by the planned, while a false negative is when a non spam call is identified as spam by the planned system. Table 1 and 2 shows the result of the experiments.

Table 1 False Negative

Number of calls	5% spammer	10 % spammer	15% spammers
200	0.02	0.025	0.055
400	0.026	0.0325	0.0575
600	0.032	0.04	0.053
800	0.038	0.049	0.061
1000	0.036	0.068	0.088

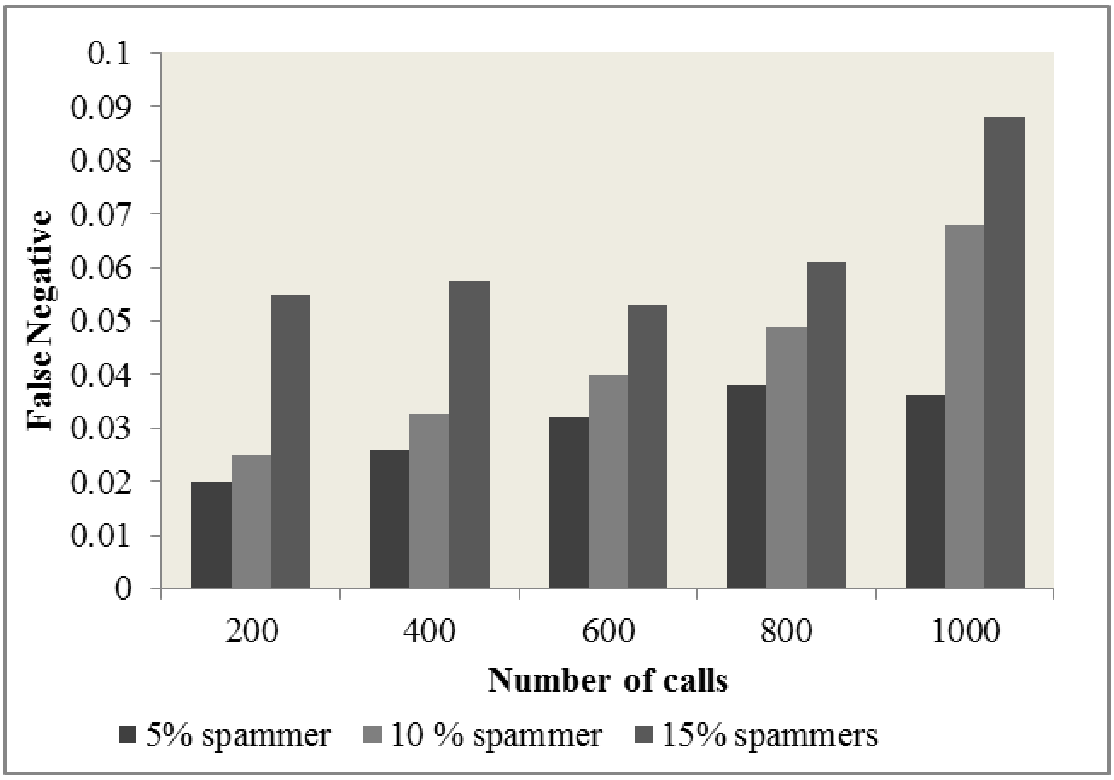

Figure 4 False Negative

From the above figure, it is experimental that false negative added to with the raise in the percentage of spammers. Also, the false negative rate added to with the raise in the number of calls.

Table 2 False Positive

Number of calls	5% spammer	10 % spammer	15% spammers
200	0.01	0.015	0.025
400	0.0075	0.0075	0.0125
600	0.0067	0.01	0.015
800	0.0075	0.00875	0.01375
1000	0.008	0.009	0.014

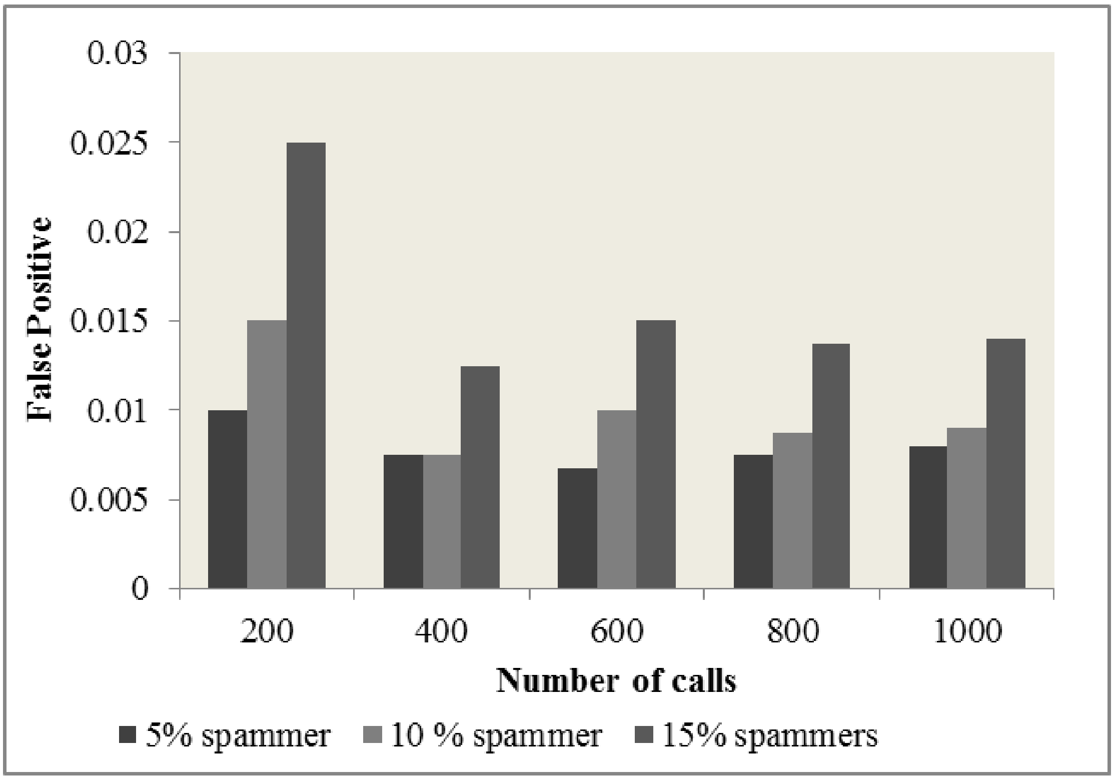

Figure 5 False Positive

5. CONCLUSION

Spam over IP telephony (SPIT) is one of the furthermost safety measures threats in VOIP. The anticipation of SPIT is one of the peak disputes for future large-scale deployments of VoIP telephony solutions. Similarly the second prevalent threat is the Man in The Middle (MITM) Attack. For example, the MITM who is in the VoIP signaling and/or media path can be simply wiretap, distract and even capture selected VoIP calls by irritating with the VoIP signaling and/or media traffic. Protecting the network using typical verification and encryption reduces the data failure; however it also reduces QOS due to elimination of authentic calls. Trust management can help developing the safety measures of VOIP. Reputation of trust in VOIP comprises data exposé decisions and key replace. We show analytically that our system significantly improves the receiving provider's assessment of SPIT tags.

REFERENCES

1. Vaishnav, C. (2006). *Voice over Internet Protocol (VoIP): the dynamics of technology and regulation* (Doctoral dissertation, Massachusetts Institute of Technology).
2. Abdelnur, H., State, R., Chrisment, I., & Popi, C. (2007, May). Assessing the security of VoIP Services. In *Integrated Network Management, 2007. IM'07. 10th IFIP/IEEE International Symposium on* (pp. 373-382). IEEE.

3. JDSU :"White Paper - VoIP Overview" - JDSU Corporation 2010
4. Kuhn, D. R., Walsh, T. J., & Fries, S. (2005). Security considerations for voice over IP systems. *NIST special publication,* 800-58.
5. Kumar, A. (2006). An overview of voice over internet protocol (voip). *Rivier College Online Academic Journal, 2*(1), 1-13.
6. Government of the HKSAR (2008). *Voice over IP security*.
7. Desantis, M. A. T. T. H. E. W. (2008). Understanding Voice over Internet Protocol (VoIP). *Retrieved November, 27,* 2011.
8. Dritsas, S., Mallios, J., Theoharidou, M., Marias, G. F., & Gritzalis, D. (2007, April). Threat analysis of the session initiation protocol regarding spam. In*Performance, Computing, and Communications Conference, 2007. IPCCC 2007. IEEE Internationa* (pp. 426-433). IEEE.
9. Wu, Y. S., Bagchi, S., Singh, N., & Wita, R. (2009, June). Spam detection in voice-over-ip calls through semi-supervised clustering. In *Dependable Systems & Networks, 2009. DSN'09. IEEE/IFIP International Conference on* (pp. 307-316). IEEE.
10. Lentzen, D., Grutzek, G., Knospe, H., & Porschmann, C. (2011, June). Content-based Detection and Prevention of Spam over IP Telephony-System Design, Prototype and First Results. In *Communications (ICC), 2011 IEEE International Conference on* (pp. 1-5). IEEE.
11. Khan, S. F., Portmann, M., & Bergmann, N. W. (2013, July). VoIP Spam Prevention. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on* (pp. 1463-1470). IEEE.
12. Chang, X., Qin, Y., Chen, Z., & Xing, B. (2012, November). ZRTP-based Trusted Transmission of VoIP Traffic and Formal Verification. In *Multimedia Information Networking and Security (MINES), 2012 Fourth International Conference on* (pp. 560-563). IEEE.
13. Falk, R., Fries, S., & Hof, H. J. (2010, August). Protecting Voice over IP Communication Using Electronic Identity Cards. In *Advances in Human-Oriented and Personalized Mechanisms, Technologies and Services (CENTRIC), 2010 Third International Conference on* (pp. 5-10). IEEE.
14. Lin, H., Xu, L., & Gao, J. (2009, April). A New Security Mechanism for SIP-Based VoIP over WMNs. In *Networks Security, Wireless Communications and Trusted Computing, 2009. NSWCTC'09. International Conference on* (Vol. 2, pp. 330-333). IEEE.
15. Thanthry, N., Gopalakrishnan, G., & Pendse, R. (2009, October). Alternate encryption scheme for VoIP traffic. In *Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on* (pp. 178-183). IEEE.
16. Deng, X., & Shore, M. (2009, March). Advanced Flooding Attack on a SIP Server. In *Availability, Reliability and Security, 2009. ARES'09. International Conference on* (pp. 647-651). IEEE.
17. Pelaez, J. C. (2009, August). Using misuse patterns for voip steganalysis. In*Database and Expert Systems Application, 2009. DEXA'09. 20th International Workshop on* (pp. 160-164). IEEE.

18. Azad, M. A., & Morla, R. (2012, June). Mitigating SPIT with Social Strength. In*Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 1393-1398). IEEE.
19. Yu, L. (2012, June). Improving Query for P2P SIP VoIP. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2012 IEEE 11th International Conference on* (pp. 1735-1740). IEEE.
20. Sattar, F., Hussain, M., & Nisar, K. (2011, July). A secure architecture for open source VoIP solutions. In *Information and Communication Technologies (ICICT), 2011 International Conference on* (pp. 1-6). IEEE.
21. Liu, L. (2011, November). Uncovering SIP vulnerabilities to DoS attacks using Coloured Petri nets. In *Trust, Security and Privacy in Computing and Communications (TrustCom), 2011 IEEE 10th International Conference on* (pp. 29-36). IEEE.
22. Dong-Huynha, T., Jennings, N., & Shadbolt, N. (2004). FIRE: An integrated trust and reputation model for open multi-agent systems. In *16th European Conference on Artificial Intelligence, Valencia, Spain* (pp. 18-22).