Realization of Call-Back Authentication (CBA) for secure web to cellular phone SMS communication

Zeeshan Shafi Khan a,b,*, Khalid Rashid c, Fahad Bin Muhaya a, Qutbuddin b, Aneel Rahim a,b

a Prince Muqrin Chair for IT Security, King Saud University, Saudi Arabia
b International Islamic University, Islamabad, Pakistan
c Comsats Institute of Information Technology, Islamabad, Pakistan

ARTICLE INFO

Keywords:
Call-Back Authentication
Pull data traffic control
Token server
SMS

ABSTRACT

In order to provide essential data services, the cellular networks have opened interface with Internet enabling communication with the users beyond the coverage of their wireless signals across the globe. Besides economical expansion of the global system for mobile communication (GSM) services, this interface has given birth to new security challenges. Especially recent research has divulged that an adversary equipped with little more than a cable modem can block all voice communication in a metropolitan area or even in entire country of the size of USA by sending enormous short message service (SMS) traffic via Internet. To overcome this threat in particular and other client–server communication problems in general, a new secure protocol, Call-Back Authentication (CBA), for web to phone SMS communication is proposed. The protocol introduces two-tier server architecture and pull data traffic control (PDTC) mechanism for secure communication. The protocol is aimed to thwart-knot malicious traffic at GSM–Internet interface gateway. The results show that the CBA protocol secures all GSM services from Internet originated SMS floods. Moreover the authentication mechanism of the CBA protocol identifies and blocks the spoofed as well as the zombie requests. The CBA server requires lesser resources to deliver SMS as compared to existing mechanism.

© 2010 Elsevier Ltd. All rights reserved.

1. Introduction

The Global System for Mobile communications (GSM) networks have global importance because of their major role in economies and social infrastructure of nations. GSM companies have expanded their service from traditional voice service to TV broadcast, Internet connectivity, email, short messaging and other value added services. Short Message Service (SMS) is considered as future driver of e-commerce [1], education [2], management and service sector due to its inherited characteristics of personal identification, low cost, location awareness and convenience of “any where any time” making it most suitable for information alerting services, marketing campaigns and real time auctions etc. Weather reports, flight, train and bus information, stock business SMS can be used for authentication purpose in information inquires, reservation services and to provide remote point of sale. For example a consumer having required balance amount in mobile phone account can purchase an item through the widely deployed automatic vending machine enabled with “dial-an-item” feature. Interface of GSM networks with Internet has enabled delivery of many services by the cellular operators at economical rate and communication beyond the range of GSM infrastructure on one hand, while inheriting the vulnerabilities and problems of Internet on the other hand.

* Corresponding author at: Prince Muqrin Chair for IT Security, King Saud University, Saudi Arabia.
E-mail addresses: zeeshanshafikhan@yahoo.com (Z.S. Khan), drkhalidrashid@comsats.edu.pk (K. Rashid), fmuhaya@ksu.edu.sa (F.B. Muhaya), qdchandio@yahoo.com (Qutbuddin), aneelrahim@ksu.edu.sa (A. Rahim).

0898-1221/$ – see front matter © 2010 Elsevier Ltd. All rights reserved.
“Web to cellular phone SMS chat”, today's popular service provided by almost all the cellular companies is more utilitarian for SMS communication for the users across the globe especially the users beyond the wireless coverage of a particular GSM operator.

Air interface of the cellular networks is a critical component because of bandwidth constraints that requires significant investment by the operators to use it. The air interface of GSM is divided into traffic channels dedicated for carrying voice & data traffic and control channels used for signaling (such as call setup/release), delivery of SMS etc. Enck et al. [3] showed that an adversary equipped with little more than a cable modem can block all voice communication in a metropolitan area or even in entire country of the size USA by sending enormous SMS traffic via Internet. Presence of this threat is a serious concern for the industrial, education, services and especially the business sector where the SMS/mobile phone are viewed as driver of future e-commerce. We proposed a new secure protocol to overcome above vulnerability in particular and to resolve other client–server communication problems in general.

The remainder of this paper is organized as follows. Section 2 gives high level overview of the related work, Section 3 investigates the problem, Section 4 describes the proposed solution while Section 5 presents the results of the CBA. Section 6 describes the future directions and conclusion.

2. Related work

Rabinovich et al. presented a new protocol named as Dual Hyper Text Transfer Protocol (DHTTP) [4]. They argue that it is not feasible to establish TCP connection for small web requests. So in order to get web service from the server, client sends a Universal Datagram Protocol (UDP) request to DHTTP Server. The Server analyzes the request and decides whether to respond via UDP or TCP depending upon the size the web page requested. The main purpose of the DHTTP is to decrease the TCP tradeoff load on web server.

William Enck et al. [3] identified the vulnerabilities and risk originated from the interface of cellular network with Internet [3]. The authors have demonstrated the ability of depriving bandwidth capacity of cellular network by sending enormous malicious SMS traffic originated from Internet resulting in denial of voice as well as legitimate SMS service. They have investigated the feasibility of exploiting the vulnerability by an adversary even equipped with limited resources. They have discussed NPA/NXX, Web scraping, web interface interaction and other techniques of creating hit lists for effective attack. They have quantified that it requires about 165 and 240 SMS per second to jam to voice & SMS service of the cities Manhattan and Washington DC respectively, that translates into dialup modem bandwidth requirement for successful attack on the cities. The authors estimate 325,525 messages per second to set the entire USA’s cellular networks non-responsive. Their suggested solutions to the problem include separation of voice and data, rate limitation and resource provisioning. However major achievement of the research is identification of the problem that emphasize on finding a better and complete solution for the problem.

Serror et al. [5] have identified vulnerability in cellular networks that offer Voice & Data services like General Packet Radio Service [5]. The research reveals that Paging Channel of air interface between Base Station and the Mobile Host can be saturated by injecting User Datagram Packets (UDP) from Internet destined for the mobile hosts. The researchers have successfully attempted to increase the traffic load by 10% and identified that creating more traffic loads are also possible. The research reveals another vulnerability of GSM caused by GPRS service that could be exploited by attackers to halt the GSM network. Since the GPRS service is not simultaneously use by all users, exploitation of the vulnerability is not severe as compared to problem discussed in [3].

William Enck et al. [6] proposed a compound solution to the problem discussed in [3]. They suggested separation of voice from SMS traffic by implementing weighted fair queue that assure reserve bandwidth quota for voice and SMS thus confining the effect of attack on SMS service ensuring minimum effect on the voice traffic [6]. Their mechanism mitigates the attack and lessens its effect on the voice traffic. However the protection of the legitimate SMS and other traffic needs to be addressed. The application of the proposed mechanism results in under utilization of available bandwidth during non-attack time.

Sher et al. [7] proposed a Transport Layer security (TLS) along with the intrusion detection system to secure the IP Multimedia Subsystem (IMS) application server against various types of time dependent and time independent flooding attacks. Since Session Initiation Protocol (SIP) is mostly used with UDP so the implementation of TLS is an issue that needs to be resolved [7]. Sher et al. [8] developed an Intrusion Detection and Prevention (IDP) system to secure the IMS application servers from floods. This IDP system compares all the incoming and outgoing requests and responses with the defined rules and decides whether to forward it or not. It is very difficult to maintain a comprehensive list of rules. In this paper the main focus of the authors is on misuse detection only. The anomaly detection is ignored by the authors [8]. Moreover attack rules are same for each type of user and request. Rebahi et al. [9] described that IMS is subject to various types of denial of service attack. In order to make the IMS successful author emphasize to secure it from these attacks. Solutions to mitigate the denial of service attack are presented in the paper [9].

2.1. Role and importance of SMS in real life

Stone et al. [2] have analyzed some field results to assess the comparative popularity level of World Wide Web, Email and SMS messaging [2]. The researchers have concluded that SMS is more popular and is an effective future tool for education. Their findings highlight the importance of SMS which leads to significance of its security arrangements.
Ching et al. [10], has proposed SMS based transport information system intended to provide requisite information by transport companies to commuters about bus schedule, route and point to point travel solutions [10]. The system is able to automatically determine the sender’s location using GSM base station. On a Query SMS to system about route, schedule and availability of transport to desired destination, the commuters are replied through SMS about various options, routes, schedule of transport available and recommend solution. This research highlights potential use of SMS in travel services that again necessitate for security measures to enable its practical implementation.

Heng Xu et al. [1], have derived hypothesized success factors for emerging SMS commerce [1]. They are of the view that success of SMS commerce is positively related to infrastructure, interoperability, low cost, high penetration of mobile phones, cooperation, government support and secure platform etc. According to them guaranteed security would be the major factor of success. The research can be considered as an indirect appeal from business sector to IT sector for security arrangements to enable revolutionary development in SMS Commerce.

Ke Wan [11], has presented application of SMS in franchise retail business to enhance its competitive advantages [11]. He has comparatively analyzed SMS with other means of communication in terms of capital cost, operational cost, training cost, security, accessibility, and information volumes. The results show that SMS is best choice for franchise business if security needs are met.

Sang et al. [12], have proposed SMS application in remote controlling and monitoring of different equipment [12]. They are of the view that information can be retrieved from a database via query-SMS. The research shows significance of SMS in terms of its wide range application scope.

Kalingamudali et al. [13], have proposed Remote Controlling and Monitoring System to control electric circuitry through SMS using Microcontroller [13]. Proposed System enables authorized users to remotely ON/OFF different appliances to monitor their status through exchange of SMS messages. The research concludes that with slight modifications, the system can be applied to many applications such as remote sensing of meteorological information and vehicle security system with location finder. By inventing useful application of SMS, the research has given wide scope to SMS that indirectly necessitate for security features to enable its smooth operations.

Zerfos et al. [14] have presented a measurement study of SMS traffic i.e. short message size distribution, their arrival process, latency, number of messages sent/received by mobile phones and External Short Message Entities [14]. The results of the study show that 94.9% messages are successfully delivered and 73.2% messages reach the destination in less than 10 s. The study is based on the one week log entries of Charging Data Records. The research reveals that SMS failure ratio of 5.1% may further increase substantially in case of the problem discussed in [3].

Meng et al. [14] have examined reliability by analyzing the Charging Data Records of a nationwide cellular network. Research shows that bulk messaging can significantly affect the reliability of cellular system because bulk messages are injected into cellular network via wired links having high bandwidth as compared to wireless interface; responsible for delivery of those messages to cellular hosts [15]. They conclude that with 5.1% failure ratio under normal conditions, SMS service is not more reliable as compared to other conventional communication systems. The research reveals that the reliability of SMS communication is at high risk in case of problem discussed in [3].

3. Problem analysis

Presently SMS based services including Web-to-SMS chat service is being managed by some cellular operators through third party service providers. The clients are offered to download an application program from the web page of the cellular operator hosted by a third party service provider. The application program enables client’s communication with the server managed by the third party hereinafter called third party server acts as mediator between the client and Short Message Service Center (SMSC). Client application program establishes Transmission Control Protocol (TCP) connection and sends SMS to third party server, which forwards the same to SMSC for delivery to destination phone. Reply from cellular user travels back to client computer through the same route. Fig. 1 describes the existing architecture of sending SMS from Internet.

Recent research [3,6] has divulged vulnerability of GSM networks to Internet originated SMS bursts that can saturate the air interface of the GSM network resulting in denial of voice service to the cities of size Washington DC. Jamming of the GSM networks is considered severe problem in view of resultant impact on economies and social infrastructure of the countries throughout the world.

This critical situation is attracting the attention of the researchers of the field i.e. Computer Science to find a reasonable, viable and acceptable solution of the problem. Because of its different architecture and nature of services, Internet based defending mechanism are insufficient to protect GSM networks (Fig. 2).

Provision of security against the attack without any compromise on availability of services, change in GSM architecture, exorbitant cost and without involvement of the cellular users is the major challenge. Any solution that suggests participation of the GSM user is not acceptable because it involves the risk of customer inconvenience which is not tolerable for service providers in this competitive commercial age.

4. CBA protocol

We purpose Call Back Authentication (CBA), a new secure protocol for web–cellular phone SMS communication that operates on two-tier server (Tier-I is Token Server, Tier-II is CBA server) using Push Data Traffic Control (PDTC). The CBA is developed to mitigate the effect of SMS flood attack. Main objectives of the CBA are:
• To enable reliable and smooth web–cellular phone SMS communication.
• To bring resilience in cellular network by defending the Internet originated SMS burst attacks while simultaneously making cellular services available.
• To decrease the degree of risk involved in the use of cellular services by different businesses, industrial, scientific and service sectors.
• To confine the scope of Internet originated SMS attack to only one cellular service (i.e. Web to SMS chat) that ensures smooth operation of the other cellular services at attack time.
• To motivate the business community and IT researchers for advancement in cellular technology and its application scope.

4.1. CBA architecture

The architecture of the CBA consists of three main entities (i) SMS Client: an application program used by client to send SMS to a mobile phone using Internet (ii) Token Server: is responsible for authenticating the clients and forwarding the list of authenticated clients to Tier-II. It operates at Tier-I of the two-tier server architecture introduced by the CBA (iii) CBA Server: the Tier-II responsible to provide service to the authenticated clients. It acts as a hub between client and GSM network for exchange of SMS traffic. The CBA works using proposed PDTC Mechanism that empowers the server to PULL the data from the clients on turn by turn basis according to its capacity and current load over the GSM network instead of traditional mechanisms those allow clients to PUSH data towards server. Fig. 3 describes the block diagram of CBA architecture. In this work we contribute the following:

(i) PDTC: a new client–server communication mechanism is introduced that:
   (a) Shifts the data/traffic queue management responsibility to client machine rather than server.
Two-tier server architecture: As an enhancement to the existing client–server architecture, a revised server architecture with following components is proposed:

(a) Tier-I Server: called token server is supposed to:
   • Listen to client request via UDP.
   • Perform security/authentication checks on client requests.
   • Provide list of authentic clients to be serviced to tier-II server.

(b) Tier-IIServer: CBA server is supposed to:
   • Initiate TCP connection with the authentic clients.
   • PULL the data/traffic from the client machine’s queue.
   • Send/Receive SMS data/traffic packets to/from client machines/SMSC.

In Fig. 3 architecture of the proposed solution is shown. A web client (SMS Client) sends a login request to token server and in response receives a token which is used for the authentication of the client. This reduces the chances of IP spoofing. In the meanwhile CBA server notifies its current load and capability to the token server. Token server provides the list of the authenticated users and CBA establishes connection with those users and PULL SMS from them according to its capabilities.

4.2. Working of CBA

The working of the CBA starts with downloading the client; (an application program) from the provider’s web site by the end user as prevailing in existing systems. The client sends login request (Four words protocol command is used with each request and reply i.e. CLGN) to token server via UDP. The token server always remains in listening mode and responds client request with an 8 byte token (ST01). It keeps the record of tokens issued against IP addresses for matching with the tokens supposed to be returned back by the clients. Every client is supposed to return the token to token server (CT01). Successful match of the token serve as surety that client IP is not spoofed.
However, still the possibility cannot be ruled out that the request is generated and simple token is returned back by a compromised machine as some maleware designed for the purpose can impersonate as legitimate user. To handle this situation token server issues an image token (ST11) to the client. It is pertinent to mention at this stage that token server behaves differently at normal and abnormal traffic threshold. When the arrival rate of requests remain below the configured value, the threshold is called normal otherwise abnormal. At abnormal traffic threshold token server considers itself under attack and activates its security mode. Image token is issued at abnormal traffic threshold. Image token consists of an image with printed text that required human intervention. Incase of legitimate client, the text printed on image is read, retyped and returned back to the token server in textual format, whereas this practice is not possible for compromised machine. On successful match of image token returned by the client (CT02), token server demands requisite data from the client (SA02).

Accordingly the client returns the requisite data i.e. (i) Nick used by the client to chat (ii) Mobile number intended to chat with and (iii) a port number (CA02). After submitting these fields, the client switches itself to listening mode by opening a TCP as well as a UDP socket over the port intimated to token server. On receipt of the requisite information, the Token server adds the client in the authenticated list (SOK2).

The CBA server according to its capacity (CBQT), configured by an administrator, takes the list of authenticated clients from token server and sends an SMS (CBCN) to the target cellular number provided by the client in order to know the willingness of the cellular user for chat with the client. Incase of timeout or unwillingness response from the cellular user, the CBA intimates the client via UDP and deletes it from the list of clients to be serviced.

However, in case of unwillingness response (SM01) from the cellular user, the CBA server initiates call-back TCP connection with the client (CB01). Here; it is noteworthy that CBA never remain in listening mode that translates into zero probability of SYN flood attack on it. Now the client manages a queue for message typed by its user, as the client is not authorized to send messages to CBA server until pulled by it. The CBA server does not maintain any queue for storing SMS but rather it sends PULL signal to each client on turn-by-turn basis to pull one SMS from client (CLMG) queue and forwards to SMSC (CBMG). The CBA server discards any SMS received from the client whom the PULL signal was not issued. Upon receiving FIN request (CLFN) either from client or from cellular user, CBA server terminates the TCP connection (CBFN) and removes the client entry from the authenticated list. Fig. 3 shows the whole process of successful authentication, session setup, SMS communication and session termination.

4.3. PDTC mechanism

In traditional client–server communication, the request for information initiated by client like HTTP requests by the client is called Pull technology whereas the transmission of requisite information by the server in response to client request is called Push Technology. Our concept of PULL is different the traditional pull concept as follows:

- Pull Signal: Client (sender) is restricted from sending SMS (data) to server (receiver) until signaled (pulled) by the server.
- Data size limit: In response to pull signal by server (receiver), the client (sender) sends the data not more than the specified number of bytes (160 bytes in case of CBA protocol).

In view of our proposed PDTC mechanism, the HTTP is categorized as Push based protocol as opposite to the traditional Pull technology that declares HTTP as Pull technology based protocol.

Fig. 4 explains the success scenario of the proposed protocol where the whole working of the protocol is shown from a legitimate user’s point of view.

Every message has a 4 letters code (we will use the word command for this 4 letter code) that tells the destination about the contents of the message. Along with the code the contents of every message are shown in ( ).

4.4. Handling the replay attack

An attacker after getting simple token or image token may replay the same token. To stop these kinds of replay attacks, a security measure called authentication level is introduced in the CBA. After issuing simple token to client, token server sets the value of authentication level to zero and with every subsequent command that it receives against the simple token, authentication level is verified and incremented. In short authentication level tells the token server about what is expected next from the client. This compels the client to follow the sequence of steps as defined by the CBA.

5. Performance evaluation

To verify the performance of the CBA, we have tested it over a Network of 50 computers test bed. Two systems were used as server (one for token server, and the other for CBA server). Third system was used to run the simulator of the GSM network. The remaining 47 nodes act as clients. We designed three types of client application programs (legitimate, spoofed and zombie). Legitimate program sends a message to a destination by using the standard method defined by the CBA. In spoofed programs a user tries to send a message from a spoofed IP address, and zombie program is a kind of virus that is running on a computer without it’s owner’s willingness. Following scenarios have been tested:
5.1. Authentication rate of legitimate, zombie and spoofed requests

The authentication mechanism of the CBA does not authenticate any of the spoofed requests, where the authentication is intended for legitimate requests. All the zombie requests are allowed authentication by the CBA at normal traffic threshold (when the traffic is normal and authentication is made by issuing simple token only) but as soon as arrival rate of requests exceed the normal threshold value and touches the abnormal threshold (when token server starts issuing image token along with simple token), the token server activates its security mode and resultantly the zombie authentication rate drops to zero. Fig. 5 shows the authentication rate of legitimate, spoofed and zombie requests at normal and abnormal traffic thresholds.

5.2. Authentication of clients at normal traffic

To verify the authentication rate of legitimate, spoofed and zombie requests at normal traffic threshold, numbers of experiments were conducted. The results conclude that all the legitimate and zombie requests got authenticated but spoofed requests were not entertained by the token server. So the total number of authenticated requests is the sum of legitimate and zombie requests. Fig. 6 shows the summary of these experiments. On horizontal axis time is shown. We conducted the experiment for 10 min and every point on the horizontal axis represents a single minute.

We can see from the Fig. 5 that at normal threshold authentication rate of spoofed users was zero (0) while the legitimate and zombie clients were getting 100% authentication. At the end of the 4th minute when traffic threshold moved from normal to abnormal rate only the legitimate clients got 100% authentication. Authentication rate of the zombie clients suddenly dropped to zero. Fig. 6 is showing the number of requests authenticated. We launched 90,000 requests from the spoofed IPs, 40,000 from the zombie machines and 1000 requests from the legitimate clients. Since the experiment is conducted at normal threshold value so zombie and legitimate clients got authenticated (40,000 + 1000 = 41,000) while the requests of the spoofed users (90,000) were declined by the token server.

5.3. Authentication of clients at abnormal traffic

The above experiments are repeated at the abnormal traffic threshold. This time results were very much different as compared to the normal traffic threshold experiment. Since abnormal traffic threshold involves reading image token, retyping the text identified for return back to the CBA server, some typographical user level errors occurred which were treated zombie requests by the CBA server as appear in the results. Moreover no zombie or spoofed request was entertained
by the token server. The total number of the authenticated clients consists of the difference of legitimate requests and user level errors. Results of these experiments are presented in the Fig. 7. On horizontal axis time is shown. We conducted the experiment for 10 min and every point on the horizontal axis represents a single minute. Fig. 7 is showing the number of requests authenticated. We launched 90,000 requests from the spoofed IPs, 40,000 from the zombie machines and 1000 requests from the legitimate clients. Since the experiment is conducted at abnormal threshold value so only legitimate clients got authenticated while the requests of the spoofed and zombie users were declined by the token server. While returning the image token few of the legitimate clients returned wrong image token because of typing mistakes (user level error). So those who sent wrong image token were not authenticated by the token server. Therefore the authenticated clients were the legitimate clients excluding those who made the spelling mistakes.

5.4. Comparison of storage resources consumed by simple SMS chat server and CBA for waiting clients

A normal SMS consists of 160 bytes. When simple chat server receives an SMS it also includes phone number (normally of 11 bytes), Nick (Normally of 8 bytes) and IP address of the client that is of 4 bytes. So an SMS normally consists of 183 bytes. When client sends an SMS to the simple chat server it is stored at the server side. So the queue is established at the server that results in occupying storage space of the server.

CBA only keeps the necessary data in its queue while the SMS data is stored at the client side. CBA pulls the data from client. This feature of CBA protects it from many types of security threats including denial of service attack through data bursts or SYN flood.

The necessary data that CBA stores for each authenticated client includes IP address of the client (4 bytes), port of the client used for communication (2 bytes), nick (8 bytes) and the phone number of the other end user (11 bytes). So it totally stores 25 bytes per user. The SMS data of 160 bytes is stored at the client side. Fig. 8 presents the comparison between simple chat server and CBA with respect to the storage space consumed by the clients in waiting. For 20,000 SMS simple chat server
3500000
3000000
2500000
2000000
1500000
1000000
500000
500 1000 2000 5000 1000015000100
No of SMS Clients in Queue
20000
4000000
0
Storage Resources Consumed (Bytes)
Simple Chat Server
CBA
5.5. Comparison of TCP connection setup and chances of syn flooding attack

Whenever a TCP request is received by the server it reserves resources of almost 280 bytes for that request without considering that whether the request is coming from malicious user or from legitimate users. In our proposed solution token server receives all the requests through UDP and stores only the token and IP of that user. So in case of normal traffic it requires only 12 bytes per request (4 bytes for the IP and 8 bytes simple token) and in case of abnormal traffic threshold token server reserves the resources of 17 bytes (4 bytes for the IP, 8 bytes simple token and 5 bytes image token). When we compare these figures for large number of connections we find that the simple chat server requires far more resources as compared to the token server as shown in Fig. 9. Another achievement of this work is elimination of the syn flooding attack. Since TCP connection is initiated by the CBA server so it eliminates the chances of syn flooding attack.

In the next experiment we measured that how much bytes token server and CBA server jointly reserve in the connection setup phase. Then we compared these values with those of simple chat server. We launched 120 requests out of which 70 were launched through spoofed users, 30 from the zombie machines and 20 requests are launched from the legitimate clients. Simple chat server allocates 280 bytes to all 120 requests. The token server allocates 12 bytes in case of normal traffic and 17 bytes in case of abnormal traffic for all 120 requests. CBA server establishes the TCP connection only with the legitimate clients at abnormal traffic threshold and with the legitimate and zombie clients at normal traffic threshold. So it reserves 280 bytes for 20 users at abnormal traffic threshold and 280 bytes for 50 users at normal traffic threshold. So the total reserved bytes in case of normal traffic threshold are 15,440 and in case of abnormal traffic threshold 7640. Simple chat server requires 33,600 bytes for 120 requests which are far more as compared to our solution. Detail results of the above experiment are shown in the Fig. 10.
6. Conclusion and future work

CBA server securely transfers the SMS from web to cellular phone and blocks the attacker’s traffic at Cellular–Internet Interface Gateway. It secures all the GSM services from the Internet originated SMS flood and confines the possibility of attack to only one cellular service (i.e. Web to SMS chat). The authentication mechanism of the CBA works well to differentiate the legitimate requests from the malicious requests. The PDTC mechanism of the CBA secures the server from various types of attacks as well as reduces the load and amount of resources required at the server side. The results shows that the CBA blocks all the spoofed users while the zombie machines are blocked as soon as the image token based authentication starts. Comparison of resources consumed shows that the CBA consumes the resources very efficiently as compared to existing web–cellular phone SMS communication.

Currently the value of the normal traffic rate is configured by an administrator. In a situation where conditions are changing very rapidly, it is not feasible to manually configure the value of normal traffic rate. So in future our focus is to develop an intelligent algorithm in order the automatically configure this value. PDTC mechanism works on turn by turn basis. Turn by turn mechanism follows the principle of first in first out algorithm. In future priorities can be introduced with PDTC mechanism. Authentication level successfully handles the replay attack but the man in middle attack can be occured and cryptographic techniques can be used to handle this attack.

References