A GSM BASED SECURITY DEVICE FOR WOMEN WORKING LATE NIGHT

[1]RAMYA R[2]HARI PRASHANTH.D [3] USHA M
VIT UNIVERSITY,INDIA.

Abstract-The GSM technology used in mobile phones can be utilized to model devices like GSM transmitter using SIM card facility which can be used as a bug device for hearing indoor conversations and other espionage purposes. In this paper we utilize this aspect for modelling a security device for women which is basically a bug and the architecture was derived from existing GSM bug device and was critically modified to suit the size and functionality. We introduce certain functions for the device to suit the needs of women in case of emergency like pressing the alert button which transmits the distress call to the cop stations nearby and the cops can identify the location of the device and the distress call using location tracking of the call, and the network architecture was designed which suits the purpose. The device has the power source which can be recharged during the charging of the mobile thereby introducing a separate socket for the device in the mobile phone, which makes marketing of the device easy. The impact of the device will be higher if it were sold as a part of a mobile phone and as a whole acts as the security provider for women who works and return home late night.

Index terms-GSM Bug, MSC (Mobile Switching Centre), Location Area Identity (LAI), BSC (Base Switching Console), Micro SIM.

I INTRODUCTION

There was an increasing crime rate against women in these days and most of them were almost helpless to offer any resistant to them like molesting, kidnap, girl and women kidnapping and selling them to any other foreign countries by social elements for money etc. were some of the few examples. This technology will help them to ensure safety. A GSM is an already existing device in mobile phones but it is not efficient or too late to ensure a women's safety since one may not know what happened to the girl exactly and what the situation she is in. so if this technology was introduced one may think in two ways, the first one is ensuring the women's safety and the other one is criminals may think thrice before they could harm a girl in the fear of being caught.

This paper is organized into following:

a) System architecture
b) Network Construction
c) Power source construction
d) Using the device as USB in mobile phone
e) Secure marketing methods

II LITERATURE REVIEW

The scalable transmitter technology was initiated and widely used during the Cold war period between USA and Soviet Union. Both sides used such devices for espionage missions. In that period between 1980s-90s the few initial devices for espionage purposes has the capacity for recording a person's conversation, call monitoring systems etc. later security-on-press button systems were used in banks, Army Bunkers, Airports etc. for security purposes. But advanced security devices for public welfare were for added security especially for women is the key aspect of this research paper.

A SIM card was first introduced in mobile phones for providing unique identity for the user as well as the device [3]. The Listening and tracker Device was the name of this bug, and the main functionality of this bug is to record indoor voices and transmit it to the user's location. The user can simply insert a sim card and call to this device through another mobile phone or through Skype software and listen to the conversation [9]

Before the development of nanotechnology A SIM based bug device as in Fig 1 was used for espionage purposes by various developed countries in early 80s-90s and later nanobots in the shape of insect, or a fly were used now[7]. Drone aircraft used for aerial monitoring. But still these SIM based bug devices are widely used in developing countries [10].

The GSM technology is one of the fastest growing technologies and now it comes with 2G, 2.5G, and 3G and so on. The speed and efficiency of the device is rapidly increasing and so it's hardware [14].

ISSN: 2278 – 1323

Fig.1 GSM Transmitter BUG

Functional requirement of this device

a) A Standalone GSM based bug device for women security
b) The device must have facility to send a distress call or cancel a distress call to the cop control room and also her parents.
c) Separate buttons for sending a distress call and cancelling a distress call should be made
d) A separate socket for embedding this device inside the mobile phone
e) The device must extract its power from the mobile battery when the phone is charged, how to transfer power from one battery to another must be found.
f) A separate network architecture which is more or less equal to the GSM architecture for call transfer mechanism must be designed.
g) Risk factors and effective risk management on or before marketing the device must be analysed

III System Architecture

A. *System Architecture of GSM Security device*

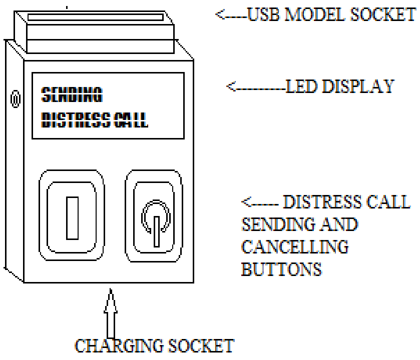

Fig.2 External architecture of the device

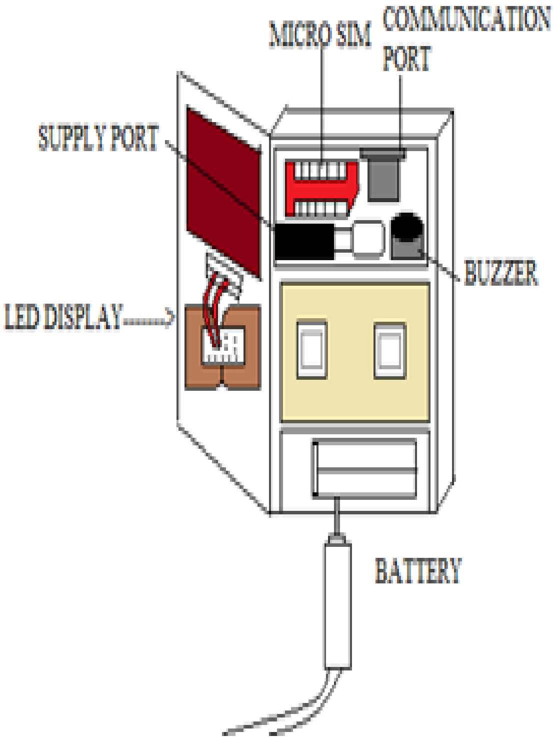

Fig.3 Internal architecture of the device

The GSM security device consists of two buttons, one for sending the distress call and another for cancelling the distress call and a USB plug-in which acts as the primary area which connects the device into the computer. A separate charging socket will be at the bottom of device. The USB socket is just for notifying whether the device is currently connected to the mobile phone or not and also the battery level of the device and it serves no other purpose. This was the external architecture of the device. The internal architecture of the device comprises of a Micro sim which acts as the basic means of equipment identity and communication, a communication port for sending and receiving signals and an LED port in which it acknowledges the user's request by displaying "SENDING DISTRESS CALL" and "CANCELLING DISTRESS CALL". The communication ports, Supply port, Button, Battery were similar architecture to the GSM spy bug. The only additional features embedded with this spy device are LED display, Distress call button and instead of using traditional sim card we are using Micro sim.

Traditional GSM device	**Proposed GSM Security device**	**Reason**
Normal sim card is used	Micro sim card is used	To compensate the proposed size
LED display is not available	LED display is available	To display status of the user's request
Has a separate charger	Charger embedded along with the mobile charger itself	Marketing of the device will be quite easy
Only has GPS and voice monitoring facility	Voice monitoring facility is not there but automatic SMS facility comes along with proposed network architecture	The main aim of the proposed architecture is to send alert from the security device to cops and parents, hence voice monitoring is not necessary
Size of the device is quite large and it's a standalone device	We introduce a separate socket for embedding this device inside the mobile phone and the overall internal architecture of the device is tightly packed	No one pay interest to buy a standalone spy device, instead if the device comes along with the mobile phone, it is easy to market all over the world quickly.

B. *Mechanism of the two distress call buttons*

Here we propose a basic speed dial mechanism for those two buttons in which the distress call button acts as the speed dial for the cop control room and also the family, the distress call button when pressed sends the distress signal which travels through a network in a fraction of second, most probably the nearby cop stations will receive the alert and they can act soon. The location of the person will be determined and the corresponding person's name and details along with the photo will be displayed in the monitoring screen of the cop control room and also a text message will be sent to the family members of the girl so that both SMS facility and Speed dial facility gets used in the process.

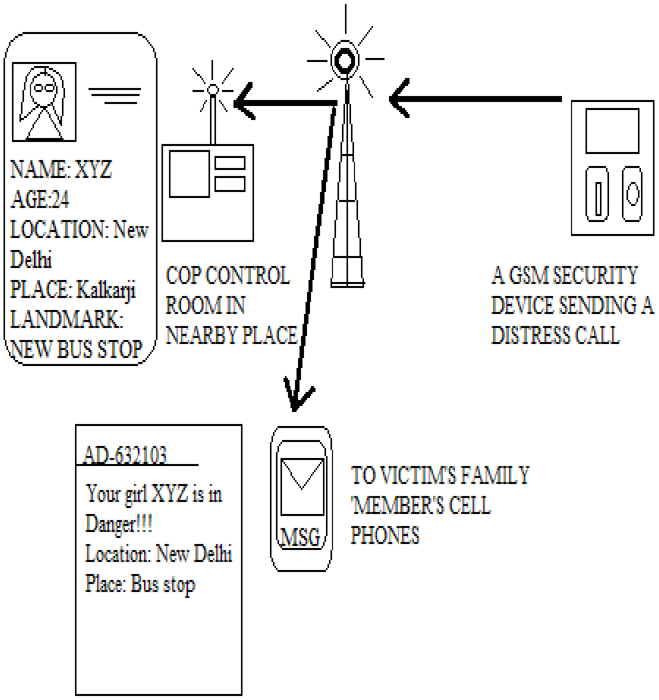
NAME: XYZ
AGE:24
LOCATION: New Delhi
PLACE: Kalkarji
LANDMARK: NEW BUS STOP
COP CONTROL ROOM IN NEARBY PLACE
A GSM SECURITY DEVICE SENDING A DISTRESS CALL
AD-632103
Your girl XYZ is in Danger!!!
Location: New Delhi
Place: Bus stop
MSG
TO VICTIM'S FAMILY 'MEMBER'S CELL PHONES

Fig.4 Outline network architecture of this device

C. *Carrying the device unnoticed*

There are many ways in which a girl can carry this device while going out in dark beneath the sleeves or hidden in pocket etc. the diagram given below illustrates one of the means of carrying the device unnoticed and outline network functionality of the GSM security device

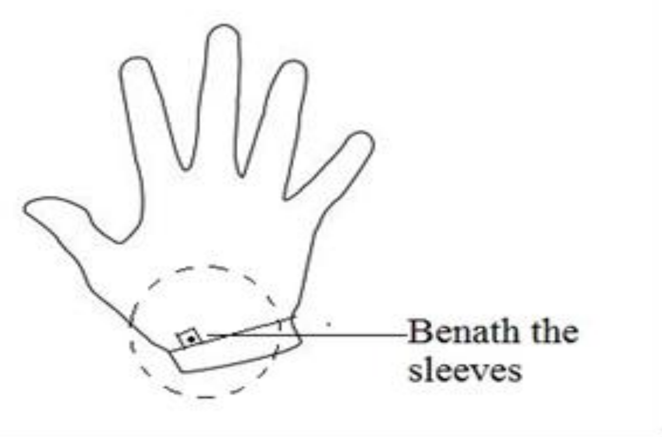

Fig.5 carrying the bug under the sleeves

IV POWER SOURCE AND CHARGING METHOD

A. *Power source construction*

What we actually need for a proper power source construction for this locator device is, we must design it in the manner that the battery of the GSM absorbs its power from the mobile phone battery when the phone is being charged. So that the suggested method of achieving this is by introducing separate 3-pin architecture for charging a battery (probably inherited feature of a mobile phone charging socket) can be introduced though that was not easy to accomplish since entire power source architecture of the mobile phone might change a little. The cheaper method of charging the device when it was inside mobile phone is, simply introduce a separate plug along with a charger wire (in the manner that two pins comes along with a single charger wire, one for mobile and the other for the GSM device)

This type of power source construction can be applied in initial stages of this introduction of this device in market and it can be upgraded later after the successful deployment of this device.

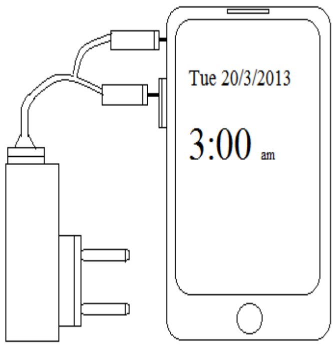

Fig.6 Proposed design of charger for flexible power supply

B. *Advantages of this type of power source construction*

Firstly we can rely on cheap and easier method of designing a power source to avoid any huge losses of investment in the research sector in case of a failure. And after the successful production of this type of power source and deploy it in market one can later think about upgrading the device. Cheaper production may reduce the cost of the device in which that was the only way to reach the people faster, even to the middle income group.

V METHOD TO EMBED THE DEVICE INSIDE THEMOBILE AS A USB

A. *Embedding this device inside a mobile phone but as a stand-alone device*

This device can be embedded inside the mobile phone just like inserting a memory card inside the respective socket. The image given below is the suggested method of inserting the GSM Device inside the mobile. The mobile phones in future can be designed in such a manner that the risks of selling the independent device can be avoided. Since mobile phones can reach the people more fast that any other means of marketing this device across the world

Above all there is a purpose why we suggest embedding this device inside the mobile phone, since there are already smart phone technology and IMI number technology, these technologies might not come in handy in case of a kidnap or a physical assault and also it is hardly the best since only after two or three days after the girl went missing can be identified that too only the location of that particular phone can be located but it is hardly a clue to locate the girl. When the girl presses a distress call button every available cop stations around the area will receive the alert and also the parents will receive the alert in that particular occasion, so that cops can react fast.

Embedding the device inside the mobile phone is not much a tough task. Initially we will try embedding this device inside a normal phone than a smart phone. A separate socket similar to the memory card socket can be introduced for this purpose. A separate socket may not be favourable in a smart phone since the thickness of a Smartphone is relatively small. In this paper we suggest a normal cell phone in which it can provide an easy space for the socket. The socket serves only as the holding space for this device and it has no other functionalities except the charging of this device when the mobile phone gets charged. The mobile battery will provide the enough power to this device so that unlike the other Facilities of the Smartphone like GPS, IMI facility etc. comes along with this device independently. The main difference between the Smartphone and this device with respect to the GPS facility is, GPS and IMI will be only used as commercial and it hardly helps in case of a crime but this spy bugging facility helps in most cases not only for identifying the person and also the person herself can send an alert signal to cops and also her parents.

The outline diagram of the suggested means of embedding this device inside the mobile phone is given below. Since we are only establishing a basic prototype of the device at the beginning a normal mobile phone is enough to demonstrate the application of this device.

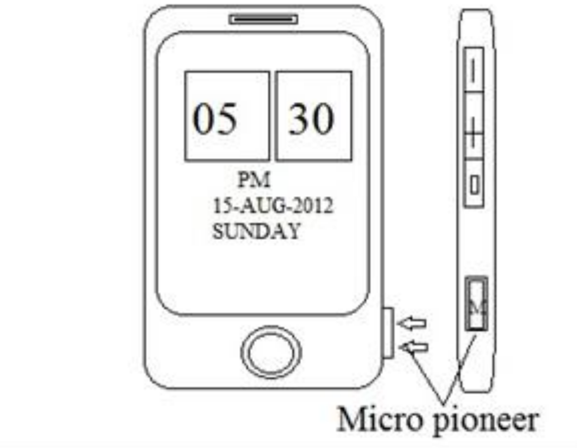

Fig.7 Method of embedding this device inside the phone

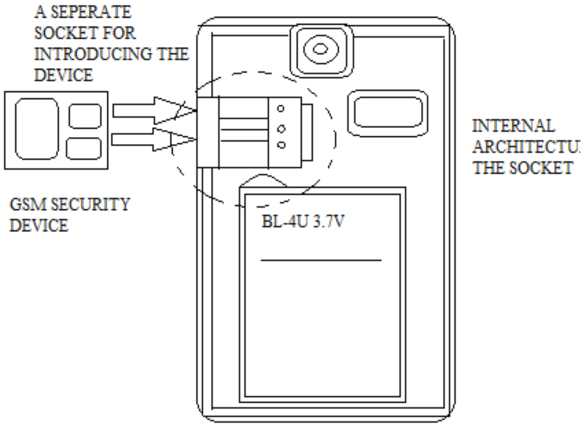
A SEPERATE SOCKET FOR INTRODUCING THE DEVICE
GSM SECURITY DEVICE
BL-4U 3.7V
INTERNAL ARCHITECTU THE SOCKET

Fig.8 Socket design

VI NETWORK ARCHITECTURE

A. *Network architecture of the device*

The GSM architecture includes the functions of the databases and messaging systems:

a. Home Location Register (HLR)
b. Visitor Location Register (VLR)
c. Equipment Identity Register (EIR)
d. Authentication Centre (AuC)
e. Gateway MSC (GMSC)

In a GSM network, the following areas are defined:

GSM Bug: GSM bug is the device which is used for locating the victim, each device is given a number that

a. Uniquely identifies the particular woman registered for the device.

b. Visitor Location Area: Each Location Area is assigned a Location Area Identity (LAI). Each Location Area is served by one or more BSCs.

c. Equipment Identity Register: This register holds the equipment ID which was registered to a unique subscriber.

d. Authentication Centre: This register respond to particular request issued by the subscriber. Which is most probably used for switching and connection termination

e. Gateway MSC: The emergency request issued by the subscriber is routed to the operator and it acts as the interface between the device and the operator who provides the service.

B. *Connection establishment between Device and network:*

When a woman makes a distress call to a PSTN telephone subscriber, the following sequence of events takes place:

a. The MSC/VLR receives the emergency request from the subscriber as he presses the emergency button.
b. The MSC/VLR identifies the device through it registers and the connection is established between the device and the operator through gateway.
c. The distress call gets automatically switched to the cops control room.
d. The cops maintain a separate register for maintaining the list of approved devices and as the device identity matches the one which was in the list of approved device list the

identity of the victim is displayed in cops control room.

e. One can make use of SMS switching service also for added security. When the identity of the victim is identified in the register an auto sms facility must be promoted to send information to the mobile phone of the victim's parents.
f. When the subscriber presses the cancel request button the connection is terminated and as long as the emergency button is active the connection will not be terminated.

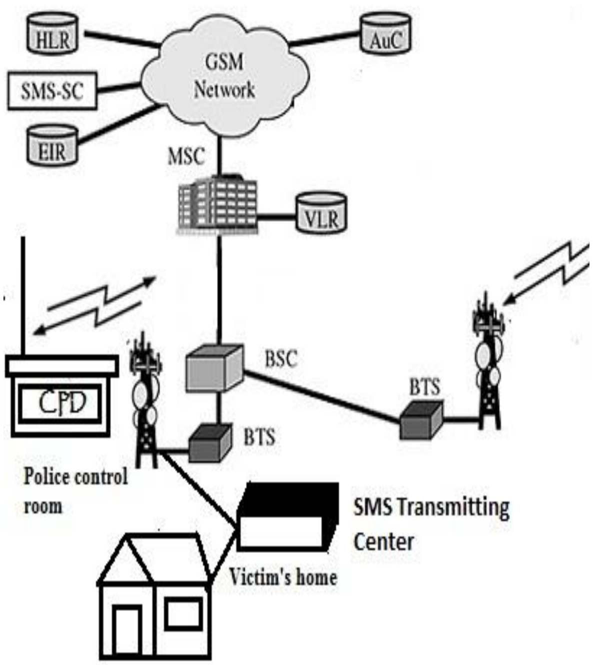

Fig.9 Network design for the GSM security device (WAN basis)

VII Secure Marketing methods

A. *Risk analysis and Risk Management*

One must take more precautions in marketing this device across the country, since there are various risk factors such as Device misuse, Making a local device and selling it in the black market etc. the table given below suggests various risk factor and how to promote effective risk management

RISK FACTOR	**SOLUTION**
Device Black market	Only registered devices can receive full support from the government, local made devices cannot access any support
Improper or accidental use of the device	The device has couple of buttons for sending distress call and also cancelling the request
Prank calls	Women using this device can register their names before using the device so that a distress call from that particular registered person will be answered and will be sent help
Gender limitations	Only women can get the device whereas for men the device will not be issued.

A. *Proper usage of this device*

The device must be sanctioned to registered users and illegal usage of this device will be strictly monitored and first of all, the network architecture and the means of communications must be fast and very much reliable. This can be achieved since 3G networks have taken its toll and high speed smart WAN were established throughout the world networking will be a handy task. And women can only use this device when they are travelling alone or in late night. Now a day in most of the developing countries offering high paid jobs, over time work is near inevitable.

VIII Conclusion

In these days of increased crime rates most probably towards the women, one may consider developing a technology which protects them from slaughter. The companies which were keen on developing Wi-Fi, Increased speed for social network connectivity, Smartphone etc. can consider developing such a technology which can ensure a women's safety. The required features and design of the GSM security device on the basis of size, network architecture, embedding method, risk factors and risk management have been discussed clearly.

IX Results

EXPERIMENT	**RESULT**
THE ARCHITECTURE OF THE DEVICE	THE SYSTEM ARCHITECTURE IS THEORETICALLY DESIGNED

MODE OF NETWORKING	A SUITABLE NETWORK CONSTRUCTION IS DESIGNED
EMBEDDING THE DEVICE IN A MOBILE PHONE	THE INTERNAL ARCHITECTURE FOR A MOBILE PHONE IN ORDER TO EMBED THE DEVICE INSIDE THE MOBILE PHONE WAS DESIGNED
SECURE MARKETING METHODS	WAYS FOR SECURE MARKETING WAS DERIVED
SOLUTIONS FOR DERIVED RISK ANALYSIS	CERTAIN SOLUTIONS FOR SUGGESTED RISK ANALYSIS IS EXPLAINED

REFERENCES

[1] IP Security Protocol, Internet Engineering Task Force (IETF). Working Group,
http://www.itef.org/html.charters/upsec-cgarter.html, 2002.

[2] Johnson, M., Revenue Assurance, Fraud and Security in 3G Telecom Services, VP Business Development Visual Wireless AB, Journal of Economic Management, Volume 1, Issue 2, 2002.

[3] Stalling, W., Cryptography and Network Security, Principles and Practice, 3rd edition, USA, Prentice Hall, 2003.

[4] Stefan, P, and Fridrich R., Authentication Schemes for 3G mobile radio, Systems, The Ninth IEEE International Symposium on, 1998.

[5] Zhang, M. and Fang, Y., Security Analysis and Enhancements of 3GPP Authentication and Key Agreement Protocol. IEEE Transactions on wireless communications, Vol. 4, No. 2, 2005.

[6] ISO/IEC 9798-4: 1999, Information technology – Security Techniques – Entity authentication – part 4: Mechanisms using a cryptographic check function.

[7] S. Hanks, T. Li, D. Farinacci and P. Traina, Generic routing encapsulation (GRE), RFC 1701 (October 1994).

[8] R. Hinden and S. Deering, IP version 6 addressing architecture, RFC 1884 (December 1995).

[9] C. Huitema, IPv6 – The New Internet Protocol (Prentice Hall PTR, Upper Saddle River, NJ, USA, 1996)

[10] The Potential of SIM Cards as an Application Platform for Smart Server Systems, Gerald Madlmayr, NFC Research Lab, Hagenberg Smart Mobility 2008.

[11] The “Simple Mobile Services” project, Project” IST 2006-034620, http://www.ist-sms.org

[12] R. Walker, G. Bartolomeo, N. Blefari-Melazzi, S. Salsano: "MEMs - Mobile Electronic Memos: efficient information capture and sharing for mobile users", Wireless World Research Forum, Meeting 18, 13-15 June 2007, Espoo, Finland.

[13] Mobile Information Device Profile 2.0, JSR 118, http://jcp.org/en/jsr/detail?id=118

[14] S. Salsano, G. Bartolomeo, C. Trubiani, N. Blefari Melazzi: “SMILE, a Simple Middleware Independent LayEr for distributed mobile applications”, IEEE Wireless Communications and Networking Conference 2008 (IEEE WCNC 2008), March 31-April 1, 2008, Las Vegas, USA

[15] D. Crockford, JSON (JavaScript Object Notation) http://www.json.org

[16] The Thinlet project, home page, http://thinlet.sourceforge.net/home.html