IOSR Journal of Engineering
May. 2012, Vol. 2(5) pp: 1259-1264

Designing a Secure Protocol for Mobile Voting Through SMS

Raghav Lakhotia, R. K. Jarial, Prashant Kumar Tiwari

***Abstract:*—This paper covers a novel scheme to solve the issue of holding fair electoral verdict indications of people in a country or in an organization through proposing the design and development of mobile voting protocol which is not only very easy to use but is also robust, secure and trusted. Due emphasis have been focused on designing a secure and globally trusted protocol to enable Indian citizens (or any other country's citizens who follows this protocol) to cast vote in their respective country's election via their GSM Mobile Phones from anywhere in the globe irrespective of their physical location. Apart from this, the motive of authors is also to extend the usage of information technology to a scheme of Green-Election (Paperless election), addresses the issues of voting-problem in remote, disturbed and sensible areas, and to suit the requirement of today's generation who, due to several problems, usually finds it difficult to go for manual vote casting.**

***Index Terms*:—Authentication Centre (AC), Home Location Register (HLR), International Mobile Subscriber Identity (IMSI), Mobile Equipment (ME), Subscriber Identity Module (SIM).**

I. INTRODUCTION

In the present world where everything is just a click away, the existing voting process in a country like India is quite hectic and insipid. It requires the voters to go out on a hot day to vote for their favourite contestant to run the democracy. The voting process also is harbinger of huge amount of national loss in terms of money as it requires the day to be off. The security losses also add to the existing problem. The process requires a change which should be friendly enough and should be authenticated as well so that user can use it without any fear and also at the same time should be prone from attacks which can harm the democracy. Voting is a vital part of the democratic process. As such, the efficiency, reliability, and security of the technologies involved are critical. Traditional voting technology includes hand-counted paper ballots. Voting is conducted in centralised or distributed places called voting booths. Voters go to voting booths and cast their votes under the supervision of authorized parties. The votes are then counted manually once the election has finished. The current voting procedure is not very efficient and mostly prone to human error. Allegations keep being raised and there are enough ways for electronic voting machine tampering, booth capturing, vote tampering, vote counting mistakes, violence and many more. These paper-based systems can result in a number of problems, including:

1. The government has to call the day off which can incur huge losses.
2. The government has to set voting booths at various places in a limited region for people to vote. This adds to the cost of voting.
3. The electronic voting machines also add to the unacceptable cost of voting.
4. The security personals which are hired for this job have to be paid heavily and even then there are chances of some tragedy at the voting booth.
5. The government has to hire volunteers to carry out this process smoothly at the voting booths.
6. The people who vote has to stay in their region of locality to vote. They are bounded and cannot go out.
7. People have to spend long hours in the queue to get their chance to vote which can be irritating and insipid on a hot day.
8. The youth who are the future of the country are many times reluctant to vote. The very thought of voting makes them sit at their home and as a case there is a gradual dip in the percentage of voting.
9. After the voting, the counting need to be done which require man power and thus adds to the voting cost of the government.
10. Also for the person to see the status of the voting, the person needs to stick to the television screen on the counting day.

II. BENEFITS OF E-VOTING

E-voting systems offer multiple advantages over traditional paper-based voting systems-advantages that increase citizen access to democratic processes and encourage participation. It not only saves a huge amount of money spent by the government for conducting voting, but also offers mobility which is the most important aspect of E-voting.

Keeping in view wider acceptability of IT in modern world in several key areas of human activity now –a- days, the proposed scheme possess a significant number of advantages that has been enumerated as follows:

A. Reduced Costs

E-voting systems reduce the materials required for printing and distributing ballots. Internet based voting, in particular, offers superior economies of scale in regard to the size of the electoral roll.

1. In case of mobile voting, the government does not need to call it a off. The voting lines will be open within a time frame which enables the user to vote as per their wish of availability of time. This will also save the huge amount of losses which government has to incur when they called the day off.
2. No need to set the voting centres for mobile voting. There will be dedicated servers which can be set at any place in the region. This saves the cost for setting voting booths.
3. No e-voting machines required. The mobile application which is portable for every mobile will act as a voting machine and thus saves a huge amount of money spend on building these voting machines.
4. No need for tight security check. Mobile voting needs no manual security and saves a huge amount as well as minimises the chances of any miss happening at the time of voting which occurs in case of e-voting.
5. No need to hire volunteers in case of mobile voting which again saves a handsome amount.

B. Mobility

In case of mobile voting, the person is not bound to stay in his region on the voting day. Since mobile feature mobility, so will mobile voting. The person can be present in any part of the world and can vote. Since the vote will be routed to local server, the user is free to travel and there is no issue of standing in the long queues to vote.

C. Increased Participation and Voting Options

There will be gradual increase in the voting percentage as the youths will also participate in a good number in case of mobile voting. This will help the national interest.

D. Instant Status Updates

The user can request a status message from the server which will send the status message instantly. This again save good amount of time and money.

E. Source of Revenue Generation

Mobile voting process will enable the government to generate huge amount of revenue instead of spending crore of rupees on voting process. Each vote cast will add Re 1 to the government account.

In this paper, we proposes an e-voting system that allows a voter to be identified using a wireless certificate without additionally registering when a user votes using his mobile terminal such as a cellular phone or a PDA. We also present a method that ensures the anonymity of voter and the confidentiality of vote content. By our mobile voting system, a voter can cast his vote more easily and conveniently than the existing e-voting using internet, within the scheduled time period anywhere even when a voter is not able to access internet on a voting day. The intention is to illustrate e-voting model and to design a voting process possessing key features.

III. BACKGROUND

A. Mobile Voting

Electronic voting systems have the potential to improve traditional voting procedures by providing added convenience and flexibility to the voter. Numerous electronic voting schemes have been proposed in the past, but most of them have failed to provide voter authentication in an efficient and transparent way. On the other hand, GSM (Global System for Mobile communications) is the most widely used mobile networking standard. There are more than one billion GSM users worldwide that represent a large user potential, not just for mobile telephony, but also for other mobile applications that exploit the mature GSM infrastructure. According to a survey conducted, India ranks second in the population chart with 1,210,193,422 (still growing) and also ranks second in the number of mobile phone usage amounting 919,170,000 mobile sets till March, 2012 which accounts for 76% of total Indian population.

B. Security Features of GSM

The services and security features to subscribers are subscriber identity confidentiality, subscriber identity authentication, user data confidentiality on physical connections, connectionless user data confidentiality and signaling information element confidentiality. They are summarized as follows:

Subscriber identity confidentiality is the property that the subscriber's real identity remains secret by protecting his International Mobile Subscriber Identity (IMSI), which is an internal subscriber identity used only by the network, and using only temporary identities for visited networks. Subscriber identity authentication is the property that ensures that the mobile subscriber who is accessing the network or using the service is the one claimed. This feature is to protect the network against unauthorized use. Data confidentiality is the property that the user information and signalling data is not disclosed to unauthorized individuals, entities or processes. This feature is to ensure the privacy of the user information.In our proposed GSM mobile voting scheme, communication between the mobile equipment and the GSM network uses standard GSM technology. Hence GSM security features apply. Among which, the subscriber identity authentication feature is particularly used in the protocol.

The subscriber identity authentication in GSM is based on a challenge response protocol. A random challenge RAND is issued when a mobile subscriber tries to access a visited network. The Authentication Centre (AC) computes a response SRES from RAND using an algorithm A3 under the control of a subscriber authentication key *Ki*, where the key *Ki* is unique to the subscriber, and is stored in the Subscriber Identity Module (SIM) on the Mobile Equipment (ME), as well as the Home Location Register (HLR). The ME also computes a response SRES from RAND as well. Then the value Recomputed by the ME is signaled to the visited network, where it is compared with the value Recomputed by the AC.

The access of the subscriber will be accepted or denied depending upon the result of comparing the two values. If the two values of SRES are the same, the mobile subscriber has been authenticated, and the connection is allowed to proceed. If the values are different, then access is denied.

IV. PROPOSED MOBILE VOTING SCHEME

A. Security Requirements for Voting Scheme

A set of voting security criteria is must for implementing the scheme. However, depending on different democratic requirements in different countries, and the different scales of electronic voting systems, security goals can vary. General security requirements include democracy, privacy, accuracy, fairness, verifiability and recoverability.

B. Democracy

All and only the authorized voters can vote, and each eligible voter can vote no more than once. Voters can also choose not to vote. To achieve democracy, voters need to be properly registered and authenticated, and then there should be a convenient way for them to cast their votes, for example, availability of different language choices, special aid for disabled voters, and proper ways for absentee voting and early voting.

C. Privacy

All votes remain secret while voting takes place and each individual vote cannot be linked by any individual to the voter who casts it. The privacy issue is paramount.

D. Accuracy

The voting result accurately reflects voters' choices. In this case, no vote can be altered, duplicated or eliminated without being detected.

E. Fairness

No partial result is available before the final result comes out. In this scheme, GSM is used for the voting system to introduce voter mobility and provide voter authentication. We start by introducing the different components of the scheme, and then the proposed voting scheme is discussed in detail.

F. The Components

1. Mobile Device with Voting Application installed
2. GSM Infrastructure
3. Counting Server

Assumption:

1. It has been assumed that mobile devices have a special button "Vote" on it with all other buttons on the keypad as in a normal mobile phone. Pressing this vote button will instruct the base station that the user is ready to vote. The further details are described in the next part.
2. In current voting procedure, every valid voter has to register themselves to Election Commission of India and get their voter ID-Card. This ID-card is used as photo identification while casting vote. While registering to election commission, user will register his/her mobile number. Firstly, the user has to activate given mobile number to enable mobile voting. The given mobile number should be a valid number which is checked at time of purchasing the SIM card by the telecom. The Indian Election Commission will now contain the following information –
   A) The Voter ID as on voter's ID-card
   B)The mobile number of the voter through which he will cast the vote

These two numbers will be unique for each user and only one vote will be cast through a single mobile number.

G. Implementation

The proposed GSM Mobile Voting scheme is divided into three phases: the pre-voting phase, the voting phase and the post-voting phase.

Pre-Voting Phase:

1. When the user wants to vote, he/she presses the "Vote" button on the handset.
2. On pressing the "Vote" button, the base station will instruct the user to switch off the handset through a service message.
3. On again switching on the handset with "Vote" button being pressed, the mobile handset will only be reserved for voting purpose and no incoming or outgoing calls can be received by the user. The exchange of messages that will take place in this phase will also be on a different frequency bandwidth than the normal frequency channel.

Voting Phase:

1. On switching the phone in Voting state, the base station will guide the user for voting process and If a user is subscribed and allowed to cast mobile vote, on election day of his/her area, user will get an SMS from Election Commission of India, having a list of candidates' name along with their parties' name and parties' symbol's name. User has to simply reply to this SMS to cast the vote.
2. This message will act as a voting machine. It is the user interface between user and the voting centre. The message contains ten digit destination field (the place where message needs to be send) which will be filled partially (eight digit) by the base station with the servers number. The last two digits will be filled by the user which will help to identify the different regions. The region code with the predefined server number will make it a ten digit number where the message will be sent from the phone of the sender. The region code will be provided by the government before voting day. The eight digit destination code is kept secret as in case of hacking, the hacker will not be able to get the destination number which makes

this application safe and secure. Also a secret key will be passed to the mobile user (this will be used to decrypt the secured encrypted SMS from election commission). The cryptography application which will be used to decrypt the SMS will be installed in the SIM earlier.

3. The message will also ask for the user voter-id number. On sending the message, the AC will check the authenticity of the user as it maintains the list of the people who are eligible to vote in a particular region along with their voter id number and SIM number (which uniquely identifies a voter).
4. If the user voter-id matches with the mobile number given by the user at the time of issuing voter-id card, then the user is granted further permission to vote and the AC sends the message in an encrypted format with a encryption key to the counting server, otherwise the vote is discarded.
5. User will get an acknowledgement SMS on the same registered number after vote acceptance.

Post-Voting Phase:

1. After the authentication check by the AC, the message is sent to the counting server with the decryption key. The user is then allowed to switch on his/her phone to work in normal condition for calling purpose.
2. The counting server, uses the decryption key sent by the AC to decrypt the message and counts the votes.

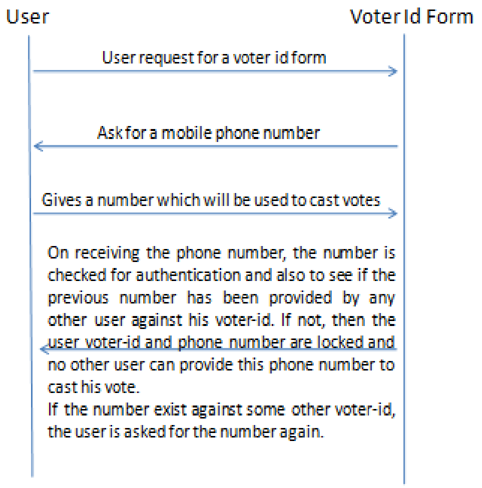
User
Voter Id Form
User request for a voter id form
Ask for a mobile phone number
Gives a number which will be used to cast votes
On receiving the phone number, the number is checked for authentication and also to see if the previous number has been provided by any other user against his voter-id. If not, then the user voter-id and phone number are locked and no other user can provide this phone number to cast his vote.
If the number exist against some other voter-id, the user is asked for the number again.

Figure 1. showing steps at time for filling form for voter id card

V. SALIENT FEATURES

It will be interesting to note that how and to what extent the method fulfils the security requirements.

1). Democracy

Only the authorized voters can vote. First, voters are authenticated through GSM, which assures that voters are who they claim to be. Further assurance is provided by Authenticating the voter-id of the user with the mobile number and IMSI number further checks the validity of the user. It is suitable for voters who travel abroad and voters who have disabilities. Also, the voting application runs on a mobile device, which can be written with different language choices, making the voting application accessible to all voters. The chance of false voting where a user press one or more buttons on the voting machine which results the vote as countless is also eliminated.

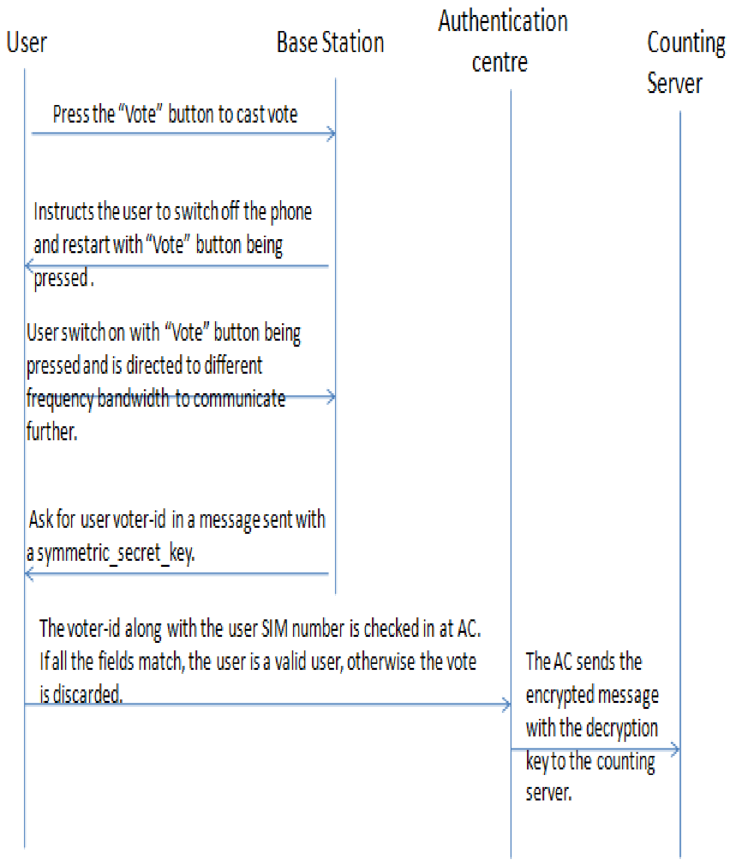
User
Base Station
Authentication centre
Counting Server
Press the "Vote" button to cast vote
Instructs the user to switch off the phone and restart with "Vote" button being pressed.
User switch on with "Vote" button being pressed and is directed to different frequency bandwidth to communicate further.
Ask for user voter-id in a message sent with a symmetric_secret_key.
The voter-id along with the user SIM number is checked in at AC. If all the fields match, the user is a valid user, otherwise the vote is discarded.
The AC sends the encrypted message with the decryption key to the counting server.

Figure 2. showing steps involved during voting

2). Security: This is the area which has to be put under special consideration. There are many levels of security checks designed for making this protocol robust and secure.

a) Secure SMS -The SMS sent to user will be secured SMS. The SMS will be encrypted with a robust symmetric encryption algorithm with a secret user's specific symmetric key. The motives that even though if the SMS will get tapped, the intruder will never be able to decrypt theisms and thus would never be able to cast a fake vote.

b) Mobile Stolen Scenario - User can contact the election commission’s help centre and after proper verification, request to block the number can be accepted. User can request election commission’s help centre to register a new mobile number for mobile-voting**.**

Privacy - All votes remain secret while the voting takes place and each individual vote cannot be linked to the voter who casts it. The proposed scheme is divided into three phases, and they are separated in time.

Accuracy - No vote can be altered, duplicated or eliminated without being detected. This helps to remove the biggest problem faced in paper voting in present scenario. Many complaints regarding people voting for others do come which is a hindrance to the democracy.

Fairness - No partial result can be known before the final result comes out. Hence, there is no partial result revealed before the final result.

Fast Access – Since during voting, the mobile is only dedicated to vote and will not be able to receive calls, the problem of channel congestion is also eliminated. If any user try to increase the traffic during voting through fake messages and calls, he/she is not allowed and only one vote will be cast through a user’s phone.

No Use of Internet – Mobile voting using internet facility have been developed but is not a major success because most of Indian population is still not comfortable using internet through mobile phone. Voting through message will be an easy and user-friendly way.

VI. DISADVANTAGES

1. Every person who is eligible to vote or is 18 years of age and above needs to get his/her mobile phone. Since only one vote is allowed by every phone so during registration, every person in a family need to give different SIM number through which the required IMSI number will be extracted by the server.
2. The protocol used for encrypting the vote message needs to be secure and attack free.

VII. CONCLUSION

The paper proposes a novel GSM mobile voting scheme, where in the GSM authentication infrastructure is used to provide voter authentication and improve voter mobility. Authentication is always a difficult requirement to fulfil for remote voting schemes, most of which apply a public-key based signature scheme for voter authentication. In our scheme, by using the existing GSM authentication infrastructure, the public-key overhead is largely reduced. The proposed scheme also enhances the security and provides more mobility and convenience to voters. In this paper, the basic structure of our GSM based mobile voting system has been presented. However, further work is needed to address the importance that has placed in trust on the AC, and also enhancing the encryption scheme and extending the GSM mobile voting scheme.

REFERENCES

[1] Abhishek Kumar, and Ashok Kumar Srivastava , “Designing and developing secure protocol for mobile voting”, *International Journal of Applied Engineering Research, Dindigul*, vol. 2, no 2, 2011

[2] Wikipedia, List of countries by number of mobile phone in use, http://en.wikipedia.org/wiki/List_of_countries_by_number_of_mobile_phones_in_use.

[3] Yang Feng, Siaw-Lynn Ng, and Scarlet Schwiderski-Grosche , “An Electronic Voting System UsingGSM Mobile Technology”, *Technical Report, RHUL–MA–2006–5*, Department of Mathematics Royal Holloway, University of London Egham, Surrey TW20 0EX, England published on 26 June 2006.

[4] Mubarak Waleed Hassan S “Design and Development of Virtual Mobile Voting Application Based Agent Classification for University Campus”, Proc. AIREET - 2011 held in NY., USA wef 21-24, 2012

[5] Keonwoo Kim, and Dowon Hong, “Electronic Voting System using Mobile Terminal”, World Academy of Science, Engineering and Technology, Proc. RRR-2007 held in UK.

Bibliography

RaghavLakhotia was born in Bareilly (Uttar Pradesh), India. He completed his Bachelor’s Degree in 2012 in Computer Science and Engineering from National Institute of Technology, Hamirpur (H.P). He is presently working at Verizon Data Services, INDIA at Chennai. He has earlier developed a online IT application for hostel room allotment and was successfully implemented for all the hostels at NIT Hamirpur for the academic session 2012-13. He has filed an application for the grant of a patent for the same.

R. K. Jarial received his Bachelor's degree [B. Sc. Engineering (Electrical)],and Master's Degree (Power Systems)in 1989 and 1992 respectively from the National Institute of Technology (NIT),Kurukshetra, Haryana, India. Since October1994, he has been working as a faculty in the department of Electrical Engineering, NIT, Hamirpur, India. His current research interest includes IT applications, Power Electronics based drives and High Voltage Engineering.

Prashant Kumar Tiwari (S'11) received his B.Tech degree in Electrical Engineering with "Honours" from U.P.T.U. Lucknow, India. He received his M. Tech degree from National Institute of Technology Hamirpur (HP)-India. Presently he is pursuing Ph.D in the Department of Electrical Engineering, National Institute of Technology Hamirpur (H.P.), India. His research interests are in the area of powe system, FACTS (Flexible AC Transmission Systems), power sector restructuring and deregulation, power system optimization and renewable energy sources.