Guarded Remittance System Employing WANET for Catastrophe Region

Mr.Bala Sundara Ganapathy.N[1], Yokeshwaran.T[2], Venugopal.S[3], Nishanth.M[4], Manoj.S[5]

[1] Assistant Professor,[2345] Students ,B-Tech, Department of Information Technology, Panimalar Engineering College, Poonamallee, Chennai,, Tamil Nadu, India.

Abstract – *In this paper, we propose an offline mobile payment system for catastrophe region utilizing WANET (Wireless Adhoc Network). The current payment system requires a fixed infrastructure network such as cellular towers, or wired networks to enable transactions. In Disaster areas, these infrastructures may not be available and impossible to get cash from banks or ATM. To overcome this issue, we provide an infrastructure less wireless network for communication which permits customers to purchase in disaster areas. Therefore we introduce a mobile payment application which enables us to make payment offline. We use multilevel endorsement mechanism to ensure guarantee payment for merchant. To reduce communication overheads we use lightweight scheme based on Bloom filter and Merkle tree. In order to make transaction easier and secured, QR codes are used consisting of digital signatures which restricts an attacker from double spending the QR. In addition with payment system, regional situation update is provided to upload their current situation such as roadblocks, floods etc.*

Key Words: WANET, Multilevel Endorser, Digital Signature, Double Spending, Merkle tree.

1. INTRODUCTION:

Now a day's usage of smart phone has increased tremendously and due to the availability of internet facility the world goes digitalized. So payments are done using online banking and other technique especially using mobile application. Since everybody carry mobile phone it makes payment easier without cash transaction. Current mobile payment adopts various technique and makes the payment system easier, secured and guaranteed. But all the available payment system's technique works only when the user has cellular connectivity or internet facility. But when there is a calamity these communication network will be destroyed or will not function properly. Even though real cash is considered to be the easiest means for carrying out a transaction it is impossible to get cash because access to the ATMs or Banks are restricted physically. Current payment system works only in the availability of the network. To overcome this situation we introduce a new way to establish communication utilizing WANET, make payment possible and shop in disaster area. We provide an android application which communicates through WANET and make transaction. We adopt various technique and strategies to make secured, easier and guaranteed payment for customer and merchant. This application does not require any fixed infrastructure for communication and the users may not know any information about the area during calamity. Moreover we provide an interface page which allows the user to view the information and upload their area situation

2. PROPOSED SYSTEM:

We proposed a payment system that will provide the infrastructure less network between User and Bank in disaster area utilizing WANET network. We use Transceivers as an intermediate for the communications between Mobiles and Banks in order to cover a wider range of communication. The Customer gets the merchant information by scanning merchant's QR code, fills payment details and passes the payment request message across the mobiles using transceivers. The QR code makes easy to fill the merchant's information and identify. For security reasons we use DES algorithm for encryption and decryption.

To transfer message in wireless medium, Base64 algorithm is used which converts the encrypted binary data into a text line format such as ASCII value. After reaching the bank the data is decrypted and it is verified. In order to provide payment guarantees we use multilevel endorsement (MLE) mechanism for a customer-to-merchant transaction. Then QR code is generated which is digitally signed that helps for authentication and moreover it restricts an attacker from double spending the QR. Bank response message reaches the customer using same strategy. Then merchant scans the received QR-code from the customer and sends information back to the Bank. Finally the QR is validated and the amount is credited to merchant. We introduced a Disaster Information center where the users can broadcast any calamity information such as Roadblocks, Bridge Collapse and flood affected areas.

3. MODULE DESCRIPTION:

3.1 Account Creation:

In this first module customer and merchant will create a bank account and sign up in the application. Then customer will deposit the amount in his account. They should give their endorser name (surety) which will be added to the account information and this will help the customer to withdraw amount from your endorser account if customer account is under minimum balance. Finally amount will be converter to bit coins (Digital currency).

3.2 Customer Payment Request:

Second module shows how the purchase is made by the customer. First the User will login with credential information like username, password and if it is valid then it opens the User profile screen. If Customer wants to purchase any item then he should scan the Merchant Shop QR code and then customer has to enter the Item name and cost of item. Then the information will be encoded with the DES Algorithm and then the encoded data will be converted into stream of bits using Base 64 Algorithm. It will be broadcasted from the customer phone and by using mobile to mobile communication the data reaches the Bank. The data is verified by the bank and if data is valid Bank generates a QR code and send it back to the customer who made the request.

3.3 Merchant Process:

In this module the received QR code will be scanned by the Merchant from the customer. The QR code contains the account information and transaction amount with digital signature. If the merchant scans the customer QR code the data is proceed to Bank through mobile communication using WANET .Bank system will check the QR code information and validates using parameters such as Date, Signature, and Time. After the successful verification, the amount will be transferred from customer to merchant account and this completed transaction will be informed to the merchant. When the transaction is completed the used QR code will become invalid to avoid Double Spending.

3.4 Regional Situation Update:

In this final module we will be providing a page where the user can upload their surrounding situation. Now all the user will be connected in WANET network. So any update made by any user will be passed to all other users. The update is made based on their location situation like Heavy rain, Road block. So this location update will be very helpful to all the people who travels or rescuers by checking the update. User can also broadcast emergency message and call for rescue which will be useful for the victims in disaster area. The Situation update can be given in three fields such as subject, place and status. Once the user update their Information, other user can view regional information in their application.

4. ARCHITECTURE DIAGRAM:

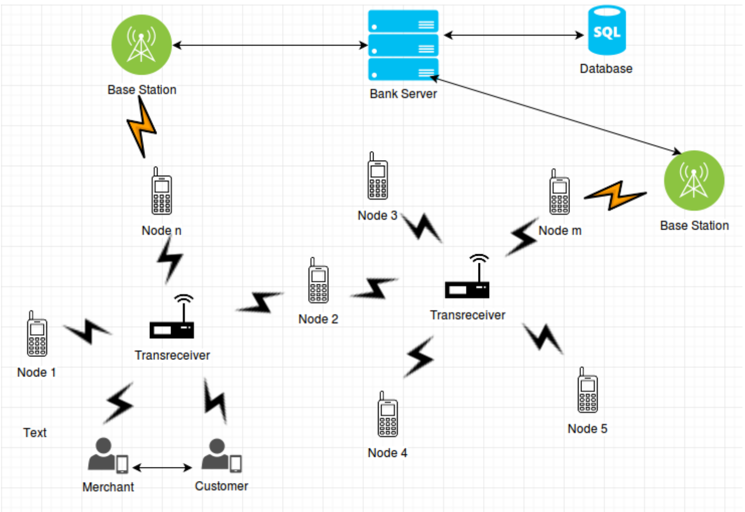

Figure 1.1 Architecture Diagram

5. ALGORITHM:

5.1 DES:

DES algorithm is a block cipher used to prevent the attack from hackers during transmission of user information. DES (Data Encryption Standard) is a symmetric key block cipher published by the National Institute of Standards and Technology (NIST).DES is an implementation of a Feistel Cipheer. It uses 16 round Fesitel structure. The block size is 64-bit. Though, key length is 64-bit, DES has an effective key length of 56bits.

General Structure of DES is depicted in the following illustration. Since DES is based on the Feistel Cipher, all that is required to specify DES is

- Initial and final permutation
- Round Function
- Key Expansion

The important significant of DES is the algorithm makes the transaction secure by using 56-bit key and 64-bit plain text. So there are 2^56 possibilities of keys which would take a decade to find the correct key using brute-force attack. It uses same algorithm for encryption and decryption.

5.2 Base64

Base64 also be referred as **P**rivacy-enhanced **E**lectronic **M**ail (PEM) is used to convert binary data into a text-like format that allows it to be transported in environments that can handle only text safely. Base64 encoding takes the original binary data and divides it into tokens of three bytes

(24 bits) and converted into printable characters from the ASCII standard. The first step is to take the three bytes (24bit) of binary data and split it into four numbers of six bits. Because the ASCII standard defines the use of seven bits, Base64 only uses 6 bits (corresponding to 2^6 = 64 characters) to ensure the encoded data is printable and none of the special characters available in ASCII are used. The ASCII characters used for Base64 are the numbers 0-9, the alphabets 26 lowercase and 26 uppercase characters plus two extra characters '+' and '/'(26+26+10+2=64).

5.3. QR Code:

QR code means Quick Response Code is the trademark for a type of Matrix Barcode (or two-dimensional barcode). A QR code uses four standardized encoding modes (numeric, alphanumeric, byte/binary, and kanji) to efficiently store data; extensions may also be used. The QR code consists of black squares arranged in a square grid on a white background which can be read by an imaging device and processed using Reed-Solomon error correction. Each of these squares is called a module. In every QR code, there are certain modules that must not be covered or edited, else the code won't scan. We specifically use IQR code.

6. HARDWARE AND SOFTWARE REQUIREMENT:

6.1 Hardware Requirement:

Windows:

Hard disk	: 250 GB and above.
Processor	: i3 and above.
RAM	: 2GB and above.

Smart Phone:

Memory	: 4GB and above.
Processor	: Dual core and above.
RAM	: 1GB and above.

6.2 Software Requirement:

Windows:

Operating System	: Windows 7 and above
Java Version	: JDK 1.7
Web Server	: Tomcat 7.0.11
Database	: MYSQL

Smart Phone:

Operating System	: Gingerbread and above.
No. of Devices	: 2(at least).

7. CONCLUSIONS

We designed an online mobile payment system using WANET to purchase product in disaster areas. The current payment system needs an online medium to enable the transaction which uses fixed infrastructure network such as cellular towers, base station etc. By using WANET can provide infrastructure less network which helps the mobile payment application to work in offline mode. So the developed application allows the user to shop even in disaster areas which reduces the fear of people from purchasing essential goods.

ACKNOWLEDGEMENT

A project of this magnitude and nature requires kind co-operation and support from many, for successful completion . We wish to express our sincere thanks to all those who were involved in the completion of this project.

REFERENCES

[1] B. Ojetunde, N. Shibata, J. Gao, and M. Ito, "An endorsement-based mobile payment system for a disaster area," in *Proc. 29th IEEE Int.Conf. Adv. Inf. Netw. Appl. (AINA)*, Gwangju, South Korea, Mar. 2015, pp. 482–489.

[2] A. Mishra and K. M. Nadkarni, "Security in wireless ad hoc networks," in *The Handbook of Ad Hoc Wireless Networks*. Boca Raton, FL, USA: CRC Press, 2003, ch. 30, pp. 499–549.

[3] W. Li, Q. Wen, Q. Su, and Z. Jin, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network," *Comput. Commun.*, vol. 35, no. 2, pp. 188–195, Jan. 2012.

[4] X. Dai, O. Ayoade, and J. Grundy, "Off-line micro-payment protocol for multiple vendors in mobile commerce," in *Proc. 7th Int. Conf. Parallel Distrib. Comput. Appl. Technol. (PDCAT)*, Taipei, Taiwan, 2006, pp. 197–202

[5] V. Patil and R. K. Shyamasundar, "An efficient, secure and delegable micro-payment system," in *Proc. IEEE Int. Conf. e-Technol. e-Commerce e-Service (EEE)*, Taipei, Taiwan, Mar. 2004, pp. 394–404.