

E-WALLET PAYMENT SYSTEM UTILIZING MANET IN DISASTER AREA

M.Bavani¹, S.Chitra², R.Ramya³

^{1,2} Final Year CSE students, ³ Assistant Professor, CSE

Thiruvalluvar College of Engineering & Technology, Vandavasi, Tamil Nadu.
bavanisumi@gmail.com¹, chitrasekar211@gmail.com², ramyar.ramu@gmail.com³

ABSTRACT-A mobile Ad-hoc Network (MANET) , also known as ad-hoc network, is a configuring self-continuously self-configuring infrastructure-less network of device connected wirelessly. The utility of MANET during disaster recovery is well-known. Dynamic network offer particular advantages in post-disaster corcumstance, permitting first responds to prioirtize the use humanitarion and repair resources in emergency situations cost by extreme weather such as earth quakes, hurricanes, floods and snowstrums. Real time data and information sharng has been extrantee from P2P communication to MANET. Having an infrastructure-less and de-centralized features, MANET is well suited to bring the network that has been collopse of a disaster. BY using MANET, we proposed a mobile payment system in disaster area have the potential to provide electronic transaction for people purchasing recovery goods. However, existing payment system require the needed communication infrastructure (like wired networks and cellular network) to enable transaction, so that these system cannot be relied on in disaster area. In this paper, we introduce a new mobile payment system utilizing infrastructure-less mobile adhoc network to enable transaction that permit users to shop in disaster area. Here we proposed an endorsement-based scheme to guarantee each transaction and a scheme to provide monitoring based on location information.

Key Terms- Endorsement, Infrastructure-less, Mobile Payment system.

1. INTRODUCTION

Large scale disasters have a major and lasting social and economic impact on people, causing damage that leads to loss of human life, materials, and massive economic loss. One of such impact is leaving people in a disaster area without cash-at-hand to purchase necessities like foodstuffs, clothes, and medicine. Although real cash is considered to be the easiest means for carrying out a transaction, it may be impossible to get cash in a disaster situation since access to a bank is restricted both physically (roads may be blocked or the bank destroyed) and electronically (communication infrastructures, like wired networks and cellular networks, may fail due to an earthquake or flooding). Furthermore, existing payment systems require such communication infrastructures for transactions in a disaster area. To enable people to do transactions even in a disaster area, therefore, of vital importance to people in disaster areas is an infrastructure less mobile payment system which can utilize flexible and robust mobile adhoc networks (MANETs) formed via the widely used smart mobile devices (smart phones, etc.).

A payment system in a disaster area is essential for people to buy necessities such as groceries, clothing, and medical supplies. In this paper, we propose a mobile payment system, adopting infrastructure less mobile ad-hoc networks (MANETs), which allow users to shop in disaster areas while providing secure transactions. Specifically, we propose an endorsement-based

scheme to guarantee each transaction and thus achieve transaction validity and reliability. Our mobile payment system can also prevent collusion between two parties and reset and recover attacks by any user. Security is ensured by using location-based mutual monitoring by nearby users, avoiding thereby double spending in the system.

The proposed system is also capable of providing such services; however, since there is no access to the bank in a disaster area, the use of electronic currency for online transaction is restricted. Therefore, our secure payment system is centered on enabling offline transactions utilizing MANETs. In designing such an MANET-based payment system, the following challenges [2] should be considered.

- 1) Frequent Network Disconnection: One of the characteristic of MANET is low-power supply, this can impede a constant connection between users.
- 2) Persistent Change in Topology: Topology changes quickly in MANET as a result of node's mobility in the network thereby leading to a decrease in performance.
- 3) Inadequate Security: Secure characteristics of wireless networks are lacking in MANETs; this increases the flaws of MANETs to attacks.

In this paper, we propose a mobile payment system that utilizes self-organized MANETs to enable people to carry out a transaction in disaster areas. The main contributions are summarized as follows.

- 1) First, we propose a new mobile payment system to allow electronic commerce in disaster areas, in a situation where the bank is not accessible.
- 2) Second, we introduce an endorsement-based scheme to provide a merchant payment guarantees for a customer using multilevel-endorser scheme to sufficiently cover transaction amount.
- 3) We introduce a transaction-log-checking scheme (called event chain) to prevent double spending attack before a transaction is completed. In addition, we propose an electronic money scheme (called e-coin) for account balance checking and to prevent a predetermined number of parties (**NC**) from colluding.
- 4) We also adopt a light-weight scheme, based on techniques of Bloom filter and Merkle tree, to reduce communication overheads.
- 5) Additionally, we introduce a mutual tracking mechanism that can proof that transaction is valid and reliable.
- 6) A digitally signed photograph is proposed for authentication and to restrict an attacker from carrying out a fraudulent transaction and impersonating others.
- 7) Furthermore, we adopt a blind signature technique to protect user's privacy by ensuring that each user uses different temporary IDs in every transaction.
- 8) Finally, we evaluate the performance of our proposed secure payment system by simulation to test the usability in disaster areas. Our simulation focused on: the ratio of successful transaction completions, merchant communication overhead, the validity ratio (VR) of event chain, the size of an event chain and the effect of various parameters such as endorser density, mobility speed of nodes and density of monitoring nodes on the transaction completion ratio (TCR).

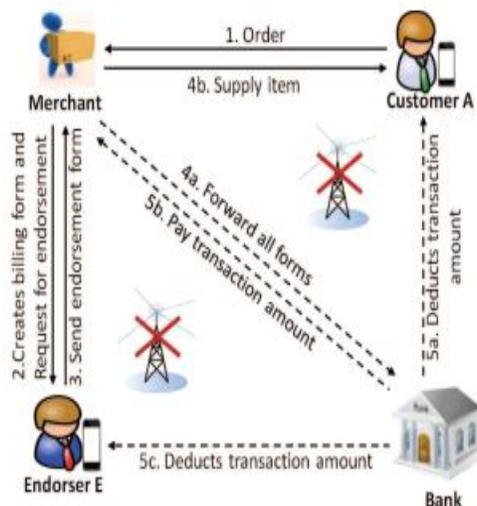
2. RELATED WORKS

As mentioned in the paper, "An endorsement-based mobile payment system for a disaster area [1]", a payment system in a disaster area is essential for people to buy essential things. However existing payment system require an effective communication with proper infrastructure. So these system can't be used destroyed due to calamities in this paper a method to communicate in the disastrous situation is given. This gives motivation to adopt endorsement based mobile Payment system in the disaster area in our paper.

Value added application in VANET come with the facility of communicating directly between the peers due to lock of internet access and hence lot of security challenges also arises. In this paper they proposed an efficient and secured payment protocol which aims at the restricted connectivity scenario in VANET. This protocol applies self-certified key agreement which can be integrated with the payment pace and their by reducing the computational and communication cost. This paper, "An efficient and secure mobile payment protocol for restricted connectivity scenarios in vehicular ad hoc network [2] ", motivates for authentication through self-certified key agreement which is very much useful for payment in disastrous environment.

In this paper "A novel proxy deposit protocol for e-cash systems [3]", a proxy deposit protocol for e-cash system is implemented. In the conventional e-cash scheme a merchant must maintain an account at the issuer for depositing their received e-cash from the customer since there will be a lot of issuer in the real world, each merchant must maintain an account at each issuers for depositing all kinds of e-cash. In order to reduce the onus of the merchant, the concept of deposit delegation protocol is introduced such that the merchant has to maintain an account at it's trading bank and delegates all deposit business to it. From this we got the motivation of minimizing that transaction scheme with proper delegation protocol.

3. SYSTEM IMPLEMENTATION



3.1 Working Principle:

Customer A sends a transaction order message to buy anything from the merchant. The merchant confirms customer A's identity (by a digitally signed photograph), creates a billing message. However, since there is no direct connection to the bank and there are no means of

confirming if Customer A has enough money in his/her account, the merchant will request of the endorser, by forwarding the billing and transaction messages to the endorser, that the endorser guarantee the transaction. The endorser forwards the endorsement message, billing message and transaction order message to the merchant. The bank confirms that the identity of all users and that all the information provided are genuine.

(a) The bank then confirms the account balance of customer A and deducts the transaction amount, (e.g. deducts \$50).

(b) The bank pays the merchant, (e.g. adds \$50 to the merchants account).

(c) However, if customer A does not have enough money to pay for the item, the money is deducted from endorser E.

4.CONCLUSION

In this paper, we proposed a new mobile payment system which utilizes infrastructure less MANETs to enable users to buy recovery goods in a disaster area. According to the endorsement mechanism, endorsers provide absolute payment security for every transaction between a customer and a merchant, therefore permitting mobile transactions in disaster areas even without direct access to the bank. Moreover, by adopting various schemes like the Bloom filter, the blind signature, the event chain plus location information-based monitoring, the proposed mobile payment system is capable of providing secure transactions, while preventing a fraudulent transaction, collusion, reset and recovery attacks, impersonation of users, double spending. The system also reduces merchant overhead and transaction completion time.

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. 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.
3. Y.-Y. Chen, J.-K. Jan, and C.-L. Chen, "A novel proxy deposit protocol for e-cash systems," *Appl. Math. Comput.*, vol. 163, no. 2, pp. 869–877, 2005.