Implication of Secure Micropayment System Using Process Oriented Structural Design by Hash chaining in Mobile Network

Chitra Kiran N.
Research Scholar
Dept of Electronics & Communication Engg.
UVCE
Bangalore, India

Dr. G. Narendra Kumar
Prof. Dept. of Electronics & Communication Engg.
UVCE
Bangalore, India

Abstract— **The proposed system presents a novel approach of designing a highly secured and robust process oriented architecture for micropayment system in wireless adhoc network. Deployment of any confidential transaction over dynamic nature of wireless adhoc network will strike a high amount of security challenges which is very difficult to identify which poses a great difficulty in designing and effective countermeasures. The current work designs the security process using hash chain and Simple Public Key Infrastructure to be implemented on newly designed digital agreement of broker along with paving new secure routing for secure m-transaction as an efficient alternative for digital coin. The system stimulates the intermediate nodes to cooperate for facilitating secure and reliable transaction from source to destination nodes. The system consists of high end encryption using hash function is also independent of any Trusted Third Party when the network topology frequency changes, thereby it is flexible, lightweight, and reliable for secure micropayment systems. The analysis result shows the system is highly robust and secure ensuring anonymity, privacy, non-repudiation offline payment system over wireless adhoc network.**

Keywords-Micropayment, M-Commerce, hash-function, offline transaction

I. INTRODUCTION

Wireless adhoc network has become one of the prime topics of research in the very recent years where majority of the research work is concentrated on restricted user-groups, where various nodes cooperate to communicate [1]. But security and energy consumption is always a never ending issue in wireless adhoc network. Although wireless adhoc network can be effectively used in wireless payment system cost effectively, but unfortunately, such technology comes with many security flaws. One of the prominent classes of payment found to be used in m-commerce recently is micropayment system [2] which is based managing small payment values. Mobile payment is defined as the process of exchanging financial values between two parties using a mobile device to pay for products or services [3]. With this new payment option, customers can pay for products and services anywhere and anytime with the comfort offered by their mobile devices. It is designed to operate with wireless technologies such as Bluetooth, Infrared or 802.11x[4]. The electronic payment system over the wireless mobile adhoc network is one of the considerable topics of research currently. Such type of network is characterized by dynamic topology, unwanted energy consumption, and obvious link breakage. Therefore creating a dedicated and secure payment system of ubiquitous type will become a very challenging task for any researchers. From the decentralized and infrastructureless types of the network, various threats might evolved due to dynamic topology caused by random mobility of the device as well as restricted resources on trusted handheld devices. In anonymous micropayment schemes, there is no connection between the payer and the payment means. In this case, the payment means should be secured by a third party vendor which is normally any financial institutions. The financial institution should ensure the reliability and the legitimacy of each coin in the network which also means that every user who wants to verify a coin should check with the financial institution. The second type of payment is in connection to the payer, where each payment mean or token should include the characteristics of the first payer. Therefore, before accepting any payment mean, a node should substantiate the first payer and verify that he owns requires the involvement of a trusted third party. Not only this, but the payee can directly redeem the payment means or use the similar token for another payment, if the micropayment mechanism allows asking for a delegation authorization. Commercially various e-payment system are in use which works on cellular network [5], but the success rate is very low due to high security threats. Majority of existing transaction systems are online and are directly dependent on a fixed cellular network with increased cost for service. Such system currently in practice has no assurity of reliability and exposed a privacy infringes implicating threats to payment systems. While electronic commerce (e-commerce) continues to have a profound impact on the global business environment, technologies and applications have begun to focus more on mobile computing and the wireless Web. With this trend comes a new set of issues and problems specifically related to wireless e-commerce. Ultimately, researchers and developers must determine what tasks users really want to perform anytime from anywhere and decide how to ensure that information and functionality to support those tasks are readily available and easily accessible [6] The communications infrastructure necessary for the wireless Internet environment is quite complex. Wireless devices are likely to remain at a disadvantage over their wired counterparts in terms of bandwidth. Limited bandwidth is a significant problem that requires organizations to rethink how users interact through a wireless device with an information system. An important issue is how to create efficient applications that can realistically work with current technology [6]. Accordingly, micropayment schemes still requires the proper designing of efficient security protocols, which could become problematical according to the quantity of the payers and the environment of the payment means and payment chains. Further, this system does not describe any robust mechanisms allowing to conclude distributed payment or pay distributed applications.

Abundant researches for e-payment system have been already proposed [7][8][9]. The researches on payment system over mobile network have been discussed in [10]. Such system has extensive deployment of expensive cryptographic protocol operations. Micropayment systems has contributed to iterative payments from a single vendor where majority of the security policies has used one-way hash functions [11] in order to generate a chain of hash values. Hash functions such as MD5/SHA are more computationally proficient in comparison to other symmetric key algorithms such as AES or asymmetric key algorithms such as RSA and allow for fast generation and verification of payment tokens [12]. But maximum of the researches comes with a security loopholes and high costing. Use of advance cryptographic protocols in such cases will only increase the memory and network overhead for high requirement of maintenance of key management. So traditional cryptography cannot be deployed in securing the communication between one to another node in wireless adhoc network. The problem of reliability of communication becomes much worst when there is a frequent changes in the network topology. This paper provides an overview of some of the relevant technologies, applications, and issues in the relatively new field of wireless e-commerce.

This research paper will provide solution for accomplishing secure and flexible e-payment system over wireless mobile adhoc network. The proposed system does not consider any online transaction like traditional system but it is designed for offline e-payment system over wireless mobile adhoc network using Simple Public Key Infrastructure (SPKI) [13]. The system integrates almost all the banking needs very securely and cost-effectively with well adaption to direct deposits, e-cheque, amount transfer etc eradicating the threats of exposing private e-payment information to illegal third party. This phenomenon will make man-in-middle attack or any unauthorized user very difficult to explore the location of effective attack as there is no central entity in the transaction path over wireless adhoc network. The proposed system considers distributed authorization controls for various modules, where one module delegates to the other about the permission.

In Section II, we will discuss about the previous research work in this area followed by Section III about electronic payment scheme in Wireless Adhoc Network. Section IV highlights processing of Micropayment system followed by proposed system Discussion in section V. In depth discussion of research methodology is done in section-VI followed by description of architecture in section-VII. Section VIII highlights the performance analysis of the conducted experiment followed by security requirement analyzation and conclusion in section-X

II. Related work

Zhi-Yuan Hu [14] has designed an innovative and practical authentication system, Anonymous Micropayments Authentication (AMA), is designed for micropayments in mobile data network. But his work has a relative drawback for common problems of authentication mechanism based on symmetric key cryptography.

Xiaoling Dai [15] has researched on micropayment protocols in offline with multiple vendors.

Min-Shiang [16] has introduce several micro-payment schemes based on one-way hash chain and review some literatures on supporting multiple payment. The author has also proposed a new micropayment scheme, which achieve the following three goals: micro-payment multiple transactions, service providers, and anonymity.

Samad [17] has proposed a trust model from user point of view and combined it with MR2 micropayment scheme and called the new scheme TMR2. This trust model is supported by micropayment provider and assures the users that they will not be charged for in case the product is not satisfactory or it is corrupt.

Sung-Ming e.t. al [18] has studied various probabilistic micropayment Scheme shows that the scheme by Rivest may reduce the administrative cost of the bank, however it brings extensive computational overhead to the merchant.

Lih-Chyau Wuu [19] has proposed a secure and efficient off-line micro payment scheme which uses coin chain technique to make coin that the verification of coin can be done quickly by hash computation. This scheme also ensures that the coins could only be used by their owner, and protects the privacy of the consumer.

Vivek Katiyar e.t. al. [20] has discussed about role of Elliptical Curve Cryptography and presents a survey on the current use of ECC in the pervasive computing environment.

Husna Osman and Hamish Taylor [21] has discussed three key design considerations in implementing a fully distributed reputation system for ad hoc m-commerce trading systems, namely relevant reputation information, its storage and reliability.

Fouzia Mousumi and Subrun Jamil [22] has described cost effective push pull services officering SMS based mobile banking concept has been illustrated for 24 hours banking convenience which helps customers stay on top of any recent changes made in their current or deposit account or loan through SMS.

Arogundade e.t. al. [23] propose an open network system which can adapt to users changing needs as well as allowing effective and secured transaction via any customers' bank account.

Partha e.t. al [24] proposes a novel approach by utilizing cancelable biometric features for securely storing the fingerprint template by generating Secured Feature Matrix and keys for cryptographic techniques applied for data Encryption or Decryption.

Mohammad Al-Fayoumi [25] discuss an important e-payment protocol namely pay-word scheme and examine its advantages and limitations, which encourages the authors to improve the scheme that keeps all characteristics intact without compromise of the security robustness

Kaylash Chaudhary e.t. al [26] have carried out an assessment of micro-payment against a non-micro-payment credit systems for file sharing applications.

Charles K. Ayo and Wilfred Isioma Ukpere [27] propose a unified (single) smart card-based ATM card with biometric-based cash dispenser for all banking transactions

Wang [28] proposes a novel payment system with smart mobile devices, wherein customers are not limited to purchase e-cash with the fixed face-value

Currently, researchers focus on the e-payment system such that electronic cash [29-34], electronic check [35, 36], electronic traveler's check [37][38] and so on.

Moreover, many researchers proposed the e-cash payment protocol [29-34], using plenty of computational resources such that exponential operation. It causes the big burden for the system. Chang and Lai [33] proposed a flexible date-attachment scheme on e-cash and Juang [35] proposed the D-cash. Curan [39] introduces some possible additional security measures which could be implemented to strengthen the overall security architecture of Bluetooth enabled devices for m-commerce applications against man-in-the middle attack and denial-of-service attacks.

Wang e.t. al [40] proposes a novel payment system with smart mobile devices, wherein customers are not limited to purchase e-cash with the fixed face-value. The amount of every transaction is deducted directly from the customer's account, eliminating the inconvenience of fixed face-value of the e-cash, and reducing online computation cost of a bank. Using a technique of trapdoor hash function to mitigate the computational cost, our system can be used with the mobile devices effectively.

Natarajan [41] introduced a system and method of extensible authentication protocols (EAPs) based on ECC and SKE with a permutation technique evolved. The permutation in our EAPs is a process of cubing a random number w.r.to a prime. These EAPs are compatible with 3G and 4G networks and no certificates exchanged during the communication.

Panjwani [42] has analyzed two token-based authentication schemes, designed for authenticating users in banking systems implemented over mobile networks. The first scheme is currently deployed in India by a mobile banking service provider named Eko with a reach of over 50,000 customers. The second scheme was proposed recently (in joint effort with Eko) to fix weaknesses in the first one, and is now being considered for deployment. Both systems rely on PINs and printed codebooks (which are unique per user) for authentication. Chaix [43] explores the economic models associated to different mobile-payment systems.

Obviously it can be seen that majority of the work is carried on wired network with much less consideration of wireless network. The issues related to dynamic topologies of wireless adhoc network is not discussed in detailed in any of the researches described above. Although there are some effective research being done in the area of payment system, but there is a huge research gap in this area with respect to wireless mobile adhoc network.

III. SCHEMA OF E-PAYMENT

According to the definition of mobile payment in mobile payment forum, mobile payment is the financial transactions for some services or good between the trading parties through mobile terminals [44]. Businessmen or service providers can transfer the regulated electronic money from their own mobile-phone-bound account to other accounts through mobile phone, with the assistance of mobile payment environment providers [44]. In comparison with online payment, the mobile payment consists of one more responsibility, namely mobile payment service provider, which is a significant position in the whole payment performance since the trading could only be completed with the vigorous cooperation of mobile communication operators mainly due to the insecurity of mobile payment and the immaturity of this field [45]. Mobile payment makes it available to conduct trading anytime and anywhere, which is the biggest advantage of this mode of payment [46]. But this system also comes with various lethal security threats posing a greatest challenge in designing a secure payment system in wireless adhoc network. Majority of the payment system currently in use consider online communication with the network and is much infrastructure dependent, which is very different scene compared to wireless mobile adhoc network. The use of digital coin is also in abundant. But it has been seen that digital coin usage generates security issues as well as privacy issues. The pre-requisites of deployment of effective and secure payment systems in wireless mobile adhoc network are as follows:

- The security of the session can be ensured working on offline mode as direct access to central server is impossible.
- The system must ensure anonymity for the user thereby protecting the real identity of user involved in the system.
- Avoid dual payment in one transaction.
- Avoid forged or illegal resources..
- Ensuring non-repudiation for the user involved, the vendors, and the bank
- Increased efficacy must be guaranteed for optimal usage of memory and resources involved..
- The system should not use much advanced hardware for deployment in order to reduce the complexity involved in maintaining security
- The system must be scalable.

IV. Micropayment System

A micropayment is a financial transaction involving a very small amount of money and usually one that occurs online [47]. One problem that has prevented their emergence is a need to keep costs for individual transactions low which is impractical when transacting such small sums even if the transaction fee is just a few cents [47]. Micropayments have to be appropriate for the transaction of non-tangible merchandise over the Internet which inflicts necessities on speed and cost of processing of the payments: delivery occurs nearly immediately on the Internet, and often in arbitrarily small pieces. On the other hand, the bottleneck in sales of tangible merchandise, management and distribution, sets a lower bound particularly for costs to remain economical. So, the evaluation criteria of micropayment systems should include [48]:

- *Ease of use*: The application must be easy to use for the clients. There is no authorization login and PIN number to be fed all the time. The customer only needs to click and to buy a page in the web page with a micropayment system in a few seconds.
- *Security*: The aim of security in the payment procedures is to prevent any group from cheating the system. For customers and external adversaries the forms of cheating security, which are detailed to payment design, are extra expenditure of coins and creation of false coins forgery during payment.
- *Anonymity*: The customer anonymity should be protected. An elementary property of physical cash is that the association between customers and their purchases is untraceable. This means that the payment systems do not allow payments to be traced without compromising the system's security. This may encourage some potential customers to start using the payment system.
- *Divisibility:* The protocol supports multiple denominations and a range of payment values.
- *Performance:* The protocol provides high-volume payment support.
- *Robustness:* The protocol is tolerant of network bottlenecks and broker/authorizer down-time.

Table 1. Comparison of E-commerce payment methods

Property	**CyberCash [48]**	**MPay [48]**	**PayWord [48]**	**NetPay [48]**
Ease of Use	Low	High	Medium	High
Security	High	Medium	Low	Medium+
Anonymity	Low	Low	Low	Medium+
Divisibility	Very High	Very High	High	High
Performance	Very Low	High	Medium	Very High
Robustness	Low	High	High	High

There is a growing need for an effective, efficient micro-payment technology for high-volume, low-value E-commerce products and services. Current macro-payment approaches do not scale to such a domain. Most existing micro-payment technologies proposed or prototyped to date suffer from problems with security, lack of anonymity and performance

V. Proposed System

The proposed system is based on the secure and reliable transaction being carried out in an offline connection in wireless adhoc network. The proposed system is standardized with respect to communication system where it facilitates ease in deployment for clients. The proposed model will amalgamate into the hierarchical transaction system which facilitates the clients to conduct transaction both in online as well as in offline connection with reliable security measures. The proposed architecture (See Figure 2) is designed for security features using simple public key infrastructure which integrates elasticity to the use of e-cheque in offline mode using digital coins. The proposed system highlights a secure micropayment system by which the system allocates a payment to all those nodes which permits relaying of the packets thereby providing service. Such types of the nodes implicate the payment agreement to pay. The payment agreement can be governed along with the uniqueness of each node in the mobile network. This can also be verified by the Trusted Third Party (TTP). Unfortunately wireless adhoc network will not support these long-lived service (payment) agreements among the nodes due to the dynamic topology of the wireless adhoc

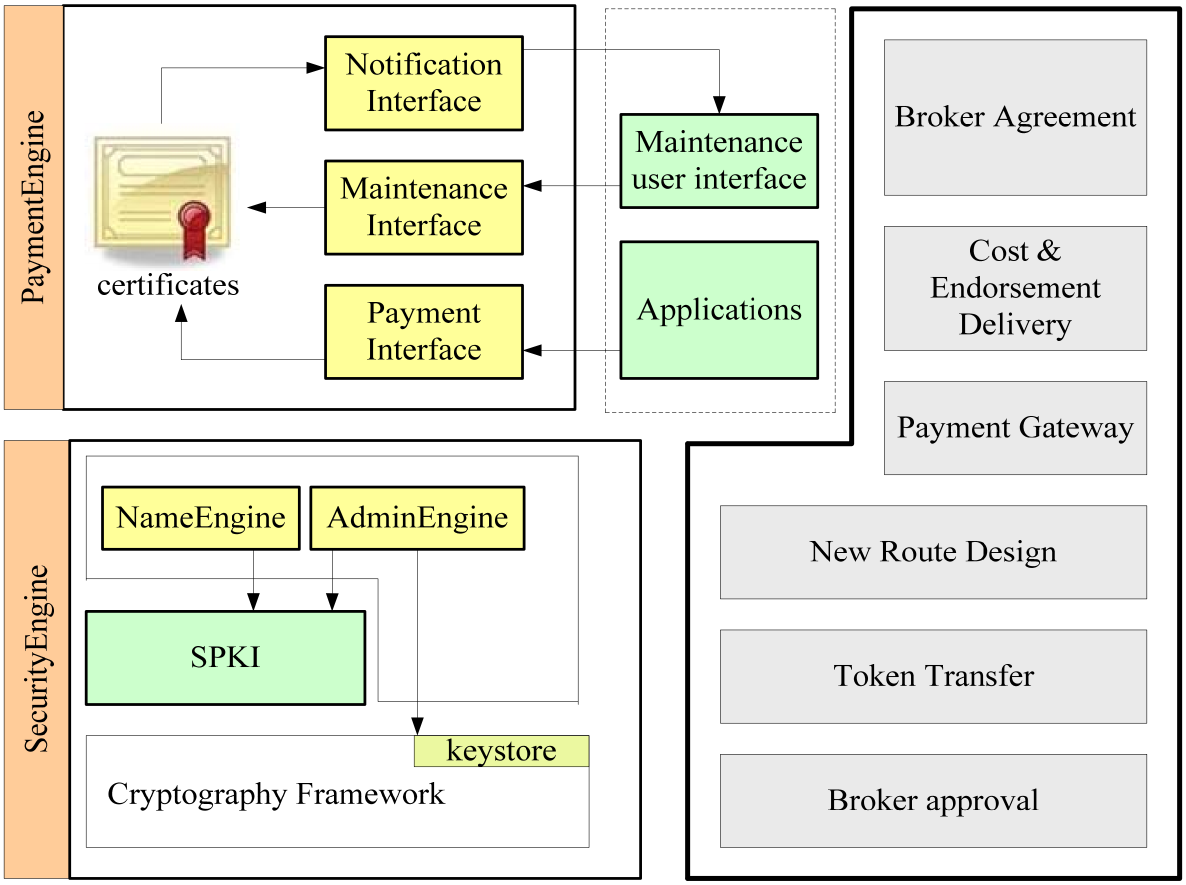

Fig.1. Architecture of the proposed structural design

network, where it is very difficult to predict the position of the nodes in next sequence of time. Therefore, there is a need of extensible as well as secure policy which allows the user to make payment to all nodes in the network without any dependency on TTP or any financial institutions to issue a new payment agreement.

The main aim of the research work is to design a secure protocol which stimulates the nodes for packet forwarding in wireless adhoc network. The objective of the proposed research journal are:

- *Verification*: The system should allow both online as well as offline validation of the payment tokens independent from any need of intermediate relay nodes.
- *Route Flexibility*: The scheme should permit selection of an most favorable route towards its destination and initiate payment to all nodes in its network. In case of route diversion, the system is independent from TTP to create a new payment agreement.
- *Cost-Effective* : Cost effective cryptographic mechanism to be applied allowing all the intermediate nodes to be able to validate the security information related to payment events in the packet.
- *Higher Security*: The system seeks to diminish all the fraudulent activities by blacklisting all the illicit users in the network.

VI. Research Methodology

The entire proposed model is design in specific set of operations to be performed by the entities involved in the secure micropayment schema using wireless adhoc network. The IETF Simple Public Key Infrastructure Working Group is tasked with producing a certificate structure and operating procedure to meet the needs of the Internet community for trust management in as easy, simple and extensible a way as possible. The SPKI is intended to provide mechanisms to support security in a wide range of Internet applications, including IPSEC protocols, encrypted electronic mail and WWW documents, payment protocols, and any other application which will require the use of public key certificates and the ability to access them. It is intended that the Simple Public Key Infrastructure will support a range of trust models. The certificate authorization of Simple Public Key Infrastructure which combines authorization to the public key is mechanized in the proposed system in order to combine authorization for mobile commercial payment to a user's key.

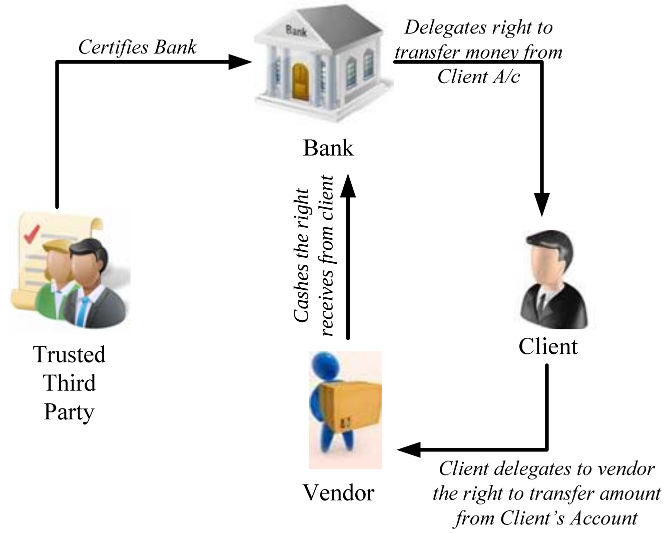
Certifies Bank
Bank
Delegates right to transfer money from Client A/c
Bank
Cashes the right receives from client
Client
Trusted Third Party
Vendor
Client delegates to vendor the right to transfer amount from Client's Account

Fig.2. Payment mechanism in proposed system

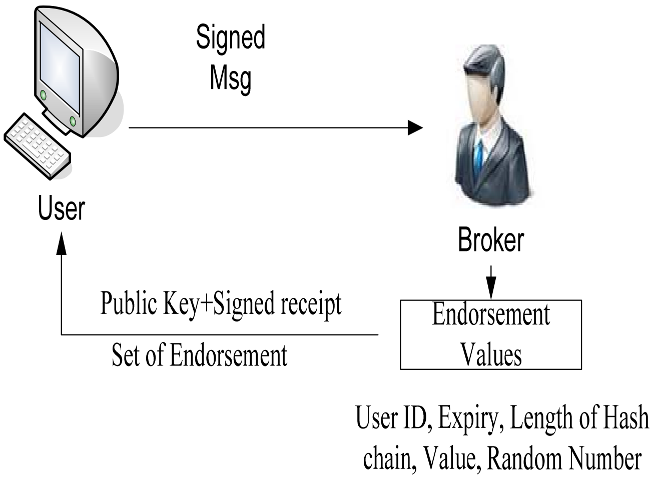
Signed Msg
User
Broker
Public Key+Signed receipt
Set of Endorsement
Endorsement Values
User ID, Expiry, Length of Hash chain, Value, Random Number

Fig.3. Broker Agreement Policy

The best feature of this model is its ability to delegate the authorization to other clients using a chain of delegates. The bank is certified by the trusted third party in the initial stage, which is done using authentication certificate for bank. In the consecutive phase, bank transmits an authorization certificate to Clients, which consist of authorization to its client C to transfer amount from client's account to the bank. The delegation flag is configured by bank which permits client to delegate this permission . Both the verification certificate along with recently designed verification certificate is transferred to client by bank. The bank identity as well as the validity of the authorization certificate of client is evaluated by client in order to check if TTP has signed the authorization certificate of bank and bank has certified that for the client. Then, client generates a new permission certificate for the vendor for transferring his rights to vendor to transfer amount from client's account. The security of the proposed system is maintained by this architecture where by implementing simple public key infrastructure by confining the rights of withdrawal. The entire cumulative certificate chain is transferred by client to vendor who analyzes its authenticity. The final stage of verification is done by bank when vendor transfer the chain to bank. The validity of the certificate is evaluated by bank to check the genuine source of the certificate (bank). After successful validation, the vendor is privileged to withdraw amount from client's account.

The authorization certificate which is frequently used consists of flag shows the validity of binding authorization and its respective delegation which is one of the prime factor of security. The proposed system assumes all the independent modules (TTP, bank, client, vendor etc) as certificate authority which is very suitable for any distributed architecture of wireless mobile adhoc network. The system reserves the chain used as it consists of confidential information related to the payment system as well as means to recognize cyber illegal users

The proposed steps are broker agreement (See Fig 3), cost and endorsement delivery, initiating payments, new route consideration, transferring tokens, and broker approval. The proposed research methodology can be explained in brief steps as following:

1. *Broker Agreement*: A broker supplies its registered and authorized user will a secure and tamper-proof token with public key pair along with highly encrypted user identity. Any micropayment schemes like credit card can be used for designing the application. The user then sends a signature message consisting of hash value and payment information which is encrypted with public key of broker. The broker generates (agreement) secret endorsement data which consists of a random number, an anchor value, length of hash chain, user-identity, and expiry of chain. These set of information is secured by private keys of broker. Therefore the broker agreement can only be deciphered by user's token. However, the security of tokens (smart cards) are not reliable as it can be deciphered, so the broker private information is appended with expiry date in order to restrict an unauthorized user in the range of mobile network to have an access on the confidential information transacted between user and broker.
2. *Cost and Endorsement Delivery*: A sender node P sends the cost request message encrypted with digital signature using their private keys to query the route of recipient node Q. All intermediate nodes attaches an certificates so that the origin node will be able to validate the digital certificates on the cost details. The data for cost reply message is returned to P. After estimating the cost involvement in routing, the encrypted broker endorsement is sent to all relay nodes in the network. These endorsements are private data, so each

user encrypt with their public key, which can be received from cost reply message. This scheme pays the intermediate routers for forwarding the packets (See Fig.4).

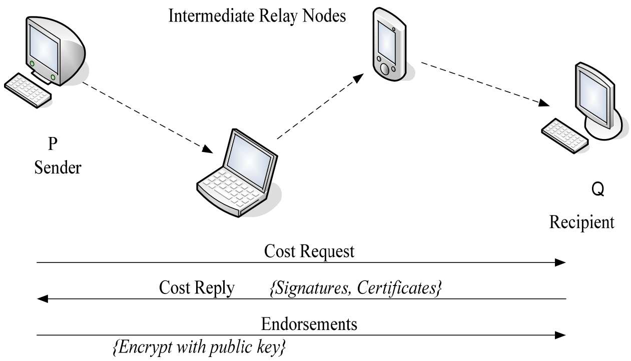

Fig.4. Endorsement-Distribution

3. *Initiating Payment*: This step is about initiating payments in the system by the user. P transmits message in his network and appends a hash token from sub-chains. The payment scheme in independent of increased used of hash values for multiple payments by the user ensuring much less network overhead. In case the intermediate relay nodes have captivated the hash values, they will not be able to decipher them without broker agreement and its respective signature.

4. *New Route Consideration*: This step is performed as wireless adhoc network quite often changes their topology dynamically. In case of new route, the system needs not to contact the any TTP. Overhead is reduced by observing the new nodes in the route and using only them for the distributing the secure endorsement.

5. *Transferring Tokens*: Here the intermediate relay node transmits the greater hash values in one chain that has spent it by the node. The user token then transmit the hash value to the consecutive broker with their endorsement digitally signed. The message and its highly encrypted contents are validated by the broker as well as issues an acknowledgement.

6. *Broker Approval*: The proposed system does support multiple brokers for reliable communication which allows any user to get associated with any broker available in the network. The user in the first network receives payment chain from the broker in that network, it assist the same user for validating the digital certificates generated by the nodes in new network when the network topology changes. The assumption to this step is that the user, broker and all the entities involved should first get themselves registered and then perform the task.

.

VII. Architecture Design

The main motive for the highlighted methodology is to build an effective and secure e-commerce system in wireless mobile adhoc network. The proposed system highlights a very flexible architecture (See Figure 1) for secure transaction in wireless mobile adhoc network.

The architecture is basically classified into two main blocks e.g. first is PaymentEngine and second is SecurityEngine. The first block i.e. PaymentEngine basically has repository of certificates for the proposed payment schemes e.g. authorization certificates, authentication certificates, account permissions etc. The first block provides an interface for notification in direct communication with updating of repository. The maintenance user interface communicates with user. The user can be considered as innermost payment service on the machine of user. The first block i.e. PaymentEngine deploys the 2nd block i.e. SecurityEngine for signing and validating chains of certificate. The security design is accomplished by using Simple Public Key Infrastructure using cryptographic framework in java which facilitates services for signing and creating chains of certificates.

According to this architecture, bank request for a digital certificate by TTP previous to any transactions to be permitted which is quite independent from any renewal. After this bank is prepared to transfer account permission to the clients assuming all the communication is done from mobile interface in wireless adhoc network. The bank again receives its public key from client and client checks his status of permission for accessing his account assuming client has an account with bank. Exactly after the previous step is accomplished, bank generates a new permission certificate and sent it to client. Now the client is prepared to communicate with vendor for payment scheme (See Fig.5).

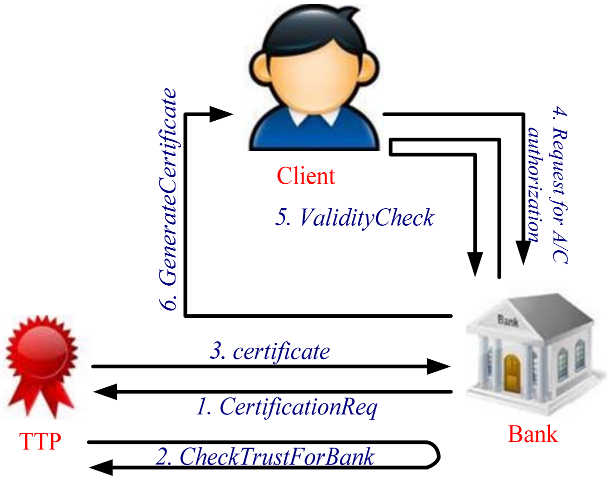

Fig.5. Permission certificate from the bank

In the second phase of the transaction (See Figure 6), when client communicates with vendor related to specific business transaction. The vendor sends a signed e-bill which includes list of TTP as there are many global TTP which user might not rely all. Client only evaluates if bank is authorized by at least one of the TTP which is conventional for vendor for secure future transaction. The communication / transaction between client and bank fails if both the party do not have certain common TTP. The transaction duration is made secure by estimating validity duration for payment. The client then generates a deposit certificate and transfer the entire chain of certificate to vendor. The vendor accepts and evaluates the entire validity of chain. It is to be noted that for security reason, the certificate is valid for only one transaction for vendor.

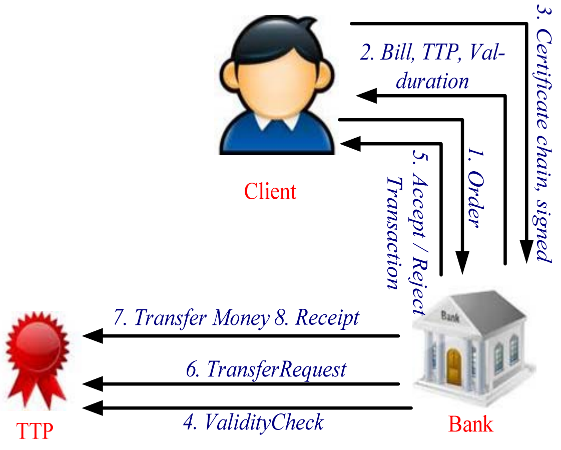
2. Bill, TTP, Val-duration
3. Certificate chain, signed
1. Order
5. Accept / Reject Transaction
Client
7. Transfer Money 8. Receipt
6. TransferRequest
4. ValidityCheck
TTP
Bank

Fig.6. Payment Interaction

One of important issue with communication on offline in wireless adhoc network is that account permission for client is feasible for being invalidated without vendor module knowing about it. In order to solve this issue, the proposed system highlights account permission with very short validity duration where bank should renew certificates frequently. Therefore if the certificate has been invalidated or rejected by the bank, than it will be subjected for acceptance offline for a very shorter duration. Therefore the proposed system with short term certificates has better security in the wireless mobile adhoc network.

VIII. Performance Analysis

The proposed system facilitates secure and reliable sets of communication with offline verification from sender to recipient node in wireless adhoc network thereby permitting a secure micropayment schemes for multiple nodes in the network by using hash functions. For providing successive endorsement distribution securely, asymmetric key are used. The proposed system is completely free from any underlying routing protocol in the wireless scenario which is very vital as routing protocols are quite dependent upon the network topologies. The long-term micropayment agreements have been eliminated because of its unsuitability in wireless adhoc network environment. Inspite of this, the cost details are securely extracted from each node in relay path to estimate a cumulative cost for forwarding the data through wireless adhoc network.

Another uniqueness in the proposed design is when a node do not have sufficient hash values for one session, then the node can be directed to some unused sub-chains by transferring a new set of endorsement. But there is a probability of loss of connection, if the system runs out of sub-chains. This phenomenon is applicable to all protocols related to micropayment system where the user registration priviledge is limited for access on the resources. The proposed system is highly favorable to the dynamic topology of wireless adhoc network as every instance the topology changes, the broker endorsement will need to be transferred to all the new nodes come across in the path. But however, it has been seen that the node mobility in such scenario as well as chain length contributes to wastage of time. However chains of higher length can be used for extreme high mobility in the network.

This section highlights the various technical requirements which are the pre-requisites for implementation of the proposed system in wireless mobile adhoc network.

A. General Security Issues

The use of robust encryption along with digital signatures assures that proposed schema is not possible to illicitly decipher without specific private keys. The payment permission certificate is created only when there is a payment request and it will embed signature of both client and vendor. This is also used for identifying the dual deployment of client's payment permission certificate. The indisputability is involuntarily accomplished as all the payments are using digital signatures. The application also ensures non- traceability as flow of the transaction from one to another module can be reconstructed as the chain of certificate consists of public key of each chain. Therefore, no third person can identify the transaction information (other than bank). The propose system therefore facilities higher dimension of privacy and security.

As the centralized service consisting of revocation list will not be accessible so invalidated certificates cannot be easily cancelled in office mode. This issue is solved by using short validity duration which needs to be renewed. Therefore the entire banking application can be integrated with the mobile application very secure in wireless mobile adhoc network in offline mode. Therefore the proposed system assures pseudonymity and restricts dual payments in one session.

B. Serviceability

The proposed system offers concrete usability and high dimension of creating a flexible and extremely secure system for offline e-commerce in wireless mobile adhoc network. There is no requirement of creating a new technology or abstraction from scratch for any clients to use this application. Clients has higher flexibility to make custom-build identity, delegate payment permission etc, which will assist in creating much organized e-payment system in wireless network. Moreover as the Simple Public Key Infrastructure has no dependency on operating system, so it will be highly feasible to deploy the application on any trusted handheld device like smart phone or mobile handset with OS and browser. The proposed system his highly at par with the ubiquitous application of banking system as the application do not consider a constant network infrastructure as it is designed on wireless mobile adhoc network. Therefore, impulsive service and usage is guaranteed at any instance.

IX. Conclusion

The proposed system presents a unique process oriented structural design for security scheme for micropayment which is completely independent of any trusted third party vendor. The proposed system has signified some of the instance of the non-cooperation of the nodes for providing services for micropayment system. The secured transaction adopted by the proposed system will allow the real-world micropayment system for guaranteed forwarding of the packets with highest reliability. The proposed system facilitates the routers to levy cost for each packet and also adapts to the dynamic network topology of the wireless adhoc network. The multiple routes to the recipient node with secure and encrypted cost of the packet is received by the node, depending on which appropriate direction and disseminated values of endorsement can be selected to each intermediate relay node. The intermediate node validates and initiates receiving tokens for forwarding the packets. The application concept is free from any dependency of the TTP in order to receive tokens for new route by intermediate routers. Using extra chains, it is able to initiate payments to the new node in the new network. Our future direction of research will include considering the trust and reputation management for providing more safe and more reliable operation in micropayments in wireless adhoc network. The proposed system also highlights a secure application for e-payment system in offline using wireless mobile adhoc network. The security of the application is governed by Simple Public Key Infrastructure. The formation of chains of certificate allows a distribution of the payment system by delegates. The designed model prevents dual expenditure in offline communication. The proposed system shows a flexible and robust solution for serviceability, security, and effectiveness in e-payment systems over wireless mobile adhoc network. The future enhancement work could be considered on design of security system based on specific attack on mobile adhoc network like DDoS or Wormhole attack, which is very common issue on pure mobile network deployment in larger scale of deployment.

REFERENCE

[1] Zygmunt J. Haas, Jing Deng, Ben Liang, Panagiotis Papadimitratos, S. Sajama,"Wireless ad hoc Networks", John Wiley & Sons, Inc, 2003

[2] Yuntsai Chou, Chiwei Lee and Jianru Chung, “Understanding m-commerce payment systems through the analytic hierarchy process”, Journal of Business Research, Volume 57, Issue 12, December 2004, Pages 1423-1430

[3] Neal Leavitt, “Payment Applications Make E-Commerce Mobile”, IEEE Computer Society, 2010

[4] Rafael Martínez-Peláez, Francisco Rico-Novella, Cristina Satizábal and Jhon J. Padilla, “Performance Analysis of Mobile Payment Protocols over the Bluetooth Wireless Network”, Whitepaper, 2008

[5] Heiko Knospe, Scarlet Schwiderski-Grosche, “Future mobile networks: ad-hoc access based on online payment with smartcards”, IEEE, 2002

[6] Peter Tarasewich, Robert C. Nickerson, Merrill Warkentin, “Wireless/Mobile E-commerce: technologies, applications, and issues”, Seventh Americas Conference on Information Systems, 2001

[7] R. Rivest and A. Shamir, "PayWord and MicroMint: Two Simple Micropayment Schemes", Security Protocols, LNCS 1189, M. Lomas, Ed., Springer-Verlag, 1997, pp. 69-87, http://theory.lcs.mit.edu/~rivest

[8] R. Hauser, M. Steiner, and M. Waidner, "Micro-payments based on iKP", in Proc. of the 14th Worldwide Congress on Computer and Communications Security Protection, Paris, 1996, pp.67-82, http://www.zurich.ibm.com

[9] W3C Micropayments Working Group, http://www.w3.org/ECommerce/Micropayments/

[10] D. O'Mahony, M. Peirce and H. Tewari, Electronic Payment Systems for E-Commerce, 2nd Ed., Artech House Publishers, Boston/London, 2001.

[11] L. Lamport, “Password Authentication with Insecure Communication”, Communications of the ACM, vol. 24, no. 11, Nov. 1981, pp. 770-72.

[12] Nachiketh R. Potlapally, Srivaths Ravi, Anand Raghunathan, Niraj K. Jha, Analyzing the energy consumption of security protocols, Proceeding ISLPED '03 Proceedings of the international symposium on Low power electronics and design, ISBN:1-58113-682-X doi>10.1145/871506.871518, 2003

[13] C. Ellison, “SPKI Requirements”, Network Working Group, Request for Comments: 2692, September 1999

[14] Zhi-Yuan Hu, Yao-Wei Liu, Xiao Hu, Jian-Hua Li, Anonymous Micropayments Authentication (AMA) in Mobile Data Network, INFOCOM 2004. Twenty-third AnnualJoint Conference of the IEEE Computer and Communications Societies Iss: 7 March 2004,

[15] Xiaoling Dai, Oluwatomi Ayoade, and John Grundy, Off-line Micro-payment Protocol for Multiple Vendors in Mobile Commerce, Proceeding PDCAT '06 Proceedings of the Seventh International Conference on Parallel and Distributed Computing, Applications and Technologies, IEEE Computer Society Washington, 2006

[16] Min-Shiang Hwang, Pei-Chen Sung, A Study of Micro-payment Based on One-Way Hash Chain, International Journal of Network Security, Vol.2, No.2, PP.81–90, Mar. 2006

[17] Samad Kardan and Mehdi Shajari, A Lightweight Buyer’s Trust Model for Micropayment Systems, WSEAS Transactions on Information Science & Applications, 2008

[18] Sung-Ming Yen, Chien-Ning Chen, Hsi-Chung Lin, Jui-Ming Wu, and Chih-Ta Lin, Improved Probabilistic Micropayment Scheme, Journal of Computers Vol.18, No.4, January 2008

[19] Lih-Chyau Wuu, Kuang-Yi Chen, Chih-Ming Lin, Off-Line Micro Payment Scheme with Dual Signature, Journal of Computers, Vol.19, No.1, April 2008

[20] Vivek Katiyar, Kamlesh Dutta, Syona Gupta, A Survey on Elliptic Curve Cryptography for Pervasive Computing Environment, International Journal of Computer Applications (0975 – 8887) Volume 11– No.10, December 2010

[21] Husna Osman, Hamish Taylor, Design of a Reputation System for M-Commerce by Ad Hoc Networking, "Design of a reputation system for m-commerce by adhoc networking," Technical Report, Dept. of Computer Science, Heriot-Watt University, 2010, pp-1-7

[22] Fouzia Mousumi, Subrun Jamil, Push Pull Services Offering SMS Based m-Banking System in Context of Bangladesh, International Arab Journal of e-Technology, Vol. 1, No. 3, January 2010

[23] Arogundade O.T, Ikotun A. Motunrayo, Olaniyi Ademola, Developing a Usage-centered e-Payment Model using Open Network System, International Journal of Computer Applications (0975 – 8887) Volume 12– No.6, December 2010

[24] Partha Pratim Ghosh, Sabyascahi Pattnaik, Gunjan Verma, Improving Existing e-payment Systems by Implementing the Concept of Cancelable Biometrics, Partha Pratim Ghosh et. al. / International Journal of Engineering Science and Technology Vol. 2(7), 2010

[25] Mohammad Al-Fayoumi, Sattar Aboud and Mustafa Al-Fayoumi, Practical E-Payment Scheme, IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 7, May 2010

[26] Kaylash Chaudhary, Xiaoling Dai and John Grundy, Experiences in Developing a Micro-payment System for Peer-to-Peer Networks, International Journal of Information Technology and Web Engineering, vol. 5, no. 1, 2010

[27] Charles K. Ayo, Wilfred Isioma Ukpere, Design of a secure unified e-payment system in Nigeria: A case study, African Journal of Business Management Vol. 4(9), pp. 1753-1760, 4 August, 2010

[28] Jian-Sen Wang, Fuw-Yi Yang, and Incheon Paik, A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices, IJCSNS International Journal of Computer Science and Network Security, VOL.11 No.6, June 2011

[29] D. Chaum, “Blind signature for untraceable payments”, In: Proceedings of advances in Cryptology, Springer-Verlag, New York, pp.199-203, 1983.

[30] W. S. Juang and H. T. Liaw, “A practical anonymous multi-authority e-cash scheme”, Applied Mathematics and Computation, Vol. 147, No. 3, pp. 699-711, 2004.

[31] Y. Y. Chen, J. K. Jan, and C. L. Chen, “A novel proxy deposit protocol for e-cash systems”, Applied Mathematics and Computation, Vol. 163, No. 2, pp. 869-877, 2005.

[32] C. L. Chen and M. H. Liu, “A traceable E-cash transfer system against blackmail via subliminal channel”, Electronic Commerce Research and Applications, Vol. 8, No. 6, pp. 327-333, 2009.

[33] C. C. Chang and Y. P. Lai, “A flexible Date-attachment Scheme on E-cash”, Computers & Security, Vol. 22, No. 2, pp.160-166, 2003.

[34] W. S. Juang, “D-cash: A flexible pre-paid e-cash scheme for date-attachment”, Electronic Commerce Research and Applications, Vol. 6, No. 1, pp. 74-80, 2007.

[35] C. C. Chang, S. C. Chang, and J. S. Lee, “An on-line electronic check system with mutual authentication”, Computers & Electrical Engineering, Vol. 35, No. 5, pp. 757-763, 2009.

[36] W. K. Chen, “Efficient on-line electronic checks”, Applied Mathematics and Computation, Vol. 162, No. 3, pp. 1259-1263, 2005.

[37] J. E. Hsien, C. C. Hsueh, and C. Y. Chen, “An electronic traveler’s check system”, Conference on Theory and Practice for Electronic Commerce, pp. 164–169, 2001.

[38] H. T. Liaw, J. F. Lin, and W. C. Wu, “A new electronic traveler’s check scheme based on one-way hash function”, Electronic Commerce Research and Applications, Vol. 6, No. 4, pp. 499-508, 2007.

[39] Kevin Curran, Shane Dempsey, “Enhancing Bluetooth security for m-commerce transactions”, Adv. Engg. Info., 2011

[40] Jian-Sen Wang, Fuw-Yi Yang, and Incheon Paik, “A Novel E-cash Payment Protocol Using Trapdoor Hash Function on Smart Mobile Devices”, IJCSNS International Journal of Computer Science and Network Security, Vol.11 No.6, June 2011

[41] Natarajan Vijayarangan, “A system and design of Extensible Authentication Protocols based on ECC and SKE mechanisms for mobile and wireless communications”, Advances in E-Activities, Information Security and Privacy, 2011

[42] Saurabh Panjwani, Prasad Naldurg, Raghav Bhaskar, “Analysis of Two Token-Based Authentication Schemes for Mobile Banking”, Technical Report of Microsoft Research, 2010

[43] Laetitia Chaix and Dominique Torre, “Different models for mobile payments, research paper, 2010

[44] Haifeng Wu, Xuan Li, Weihui Dai, Weidong Zhao, “Mobile Payment Framework Based on 3G Network, Proceedings of the Third International Symposium on Electronic Commerce and Security Workshops(ISECS ’10) Guangzhou, P. R. China, 29-31, pp. 172-175, July 2010,

[45] Mobile Payments, A White Paper by Microsoft and M-Com, 2011

[46] http://en.wikipedia.org/wiki/Mobile_payment [Accessed on 4th-Aug, 2011]

[47] http://en.wikipedia.org/wiki/Micropayment [Accessed on 30th July, 2011]

[48] Xiaoling Dai1 , John Grundy and BruceWN Lo, Comparing and contrasting micro-payment models for E-commerce systems, Info-tech and Info-net, Proceedings. ICII 2001 - Beijing. International Conferences, 2001