International Journal of Power Control Signal and Computation(IJPCSC)
Vol3. No1. Jan-Mar 2012 ISSN: 0976-268X
www.ijcns.com

Enhanced Security through Agent Based Non-Repudiation Protocol for Mobile Agents

CeronmaniSharmila V[#1], KomalaValli V[#2]
[#1] Assistant Professor (PhD), Department of IT, Hindustan University
P.O.Box No 1, Rajiv Gandhi Salai, Padur, India, 603 103
[1]csharmila@hindustanuniv.ac.in
[2]komalavadivelu@gmail.com

Abstract-In mobile communication, the key factor that affects the performance of a good security protocol is the timeliness of the security components of the transactions. Even though, there are mathematically well-established rigid security algorithms and implementation mechanisms available in the market, it is very difficult to predict the events in a mobile communication mechanism. This timeliness of the information exchange between two mobile nodes involved in any mobile wireless communication has led to various attempts to innovate good rigid security mechanisms that shall also take care of the time domain factors. Non repudiation protocols are designed in such a way that two agents were involved in transactions shall never be able to repudiate and deny the involvement at a later point of time. In this work, a non-repudiation agent based approach for resolving any conflicts in security protocols is being proposed. An evidence of a transaction is generated by wireless PKI mechanism such that User and Rights Issuer cannot repudiate sending and receiving the message respectively. User generates a mobile agent, which carries encrypted payment information to RI. The user also issues this mobile agent a proxy certificate; this certificate guarantees the binding relationship between them. One trusted third party acts as a lightweight notary for evidence generation.

Keywords -Mobile agent, Non-repudiation, WPKI, Digital rights management, Proxy certificate, Broker

1.INTRODUCTION

When a user sends some message to a rights issuer, neither User nor Right Issuer can deny having participated in this transaction. An evidence of a transaction is generated by wireless PKI mechanism such that User and Right Issuer cannot repudiate sending and receiving the message respectively. User generates a mobile agent which carries encrypted payment information to Right Issuer. This mobile agent is also issued a proxy certificate by User; this certificate guarantees the binding relationship between them. So here one trusted third party acts as a lightweight notary for evidence generation. And advantage of this agent-based non-repudiation protocol is to reduce inconvenience for mobile clients such as connection time; it causes difficulty for fair transaction for mobile Digital Rights Management. These were ensured by Non-repudiation of a mobile digital rights management.

Wireless device which communicates with application servers over the air are highly exposed to potential security threats. They enhanced security and authenticity services for mobile transactions which are not properly supported by the original GSM and UMTS security mechanism. For example Stach, Park, and Makkai. More over the application increases, further sensitive services such as payment and billing are needed. This scheme can provide non-repudiation billing services based on digital signatures. The main purpose of non-repudiation is to collect, maintain, make available and validate irrefutable evidence concerning a claimed event or action. Any evidence has to be verified by some fair arbitrator once dispute arises.

We propose an agent-based architecture and protocol to implement the non-repudiation mechanism over the mobile application systems, which includes the digital right management (DRM); this will also improve the security mechanismsof those existing electronic invoice systems. On the other hand, mobile applications need to be user friendly and convenient for mobile client through their mobile handset; this investigation leads to research for agent-based mobile applications.

Digital rights management (DRM) is a term for access control technologies that are used by hardware manufacturers, publishers, copyright holders and individuals to limit the use of digital content and devices. Many multimedia contents are distributed without any copyright protection via digitalization and communication network. The term is used to describe any technology that inhibits uses of digital content that is not desired or intended by the content provider. The term does not generally refer to other forms of copy protection, which can be circumvented without modifying the file or device, such as serial numbers or key files. It can also refer to restrictions associated with specific instances of digital works or devices.

In this paper, we show how to establish a simpleagent-based protocol integrated existing DRM architecture basedon the OMA (open mobile alliance) DRM specification. This protocolprovides the secure mechanism between the mobile user andthe right issuer through the mobile network provider, while they are exchanging a Right Object according to agreed purchase order. Non-repudiation services must ensure that when

mobile consumer U sends some content right request to rights issuer over a network, neither User nor Right Issuer can deny having participated in a part or the whole of this transaction. The basic idea is the following: an evidence of origin (EOO) is generated for U and an evidence of receipt (EOR) is generated for RI. In general, evidences are generated via PKI-based digital signatures. Disputes arise over the origin or the receipt of messages. For the case of origin dispute, User denies sending message while Right Issuer claims having received it. As for the receipt dispute, Right Issuer denies receiving any message while User claims were having sent it.

The architecture for mobile digital right management system is composed of the following entities: a user represented by mobile equipment (ME), WPKI, a content provider and corresponding (digital) rights issuer, a bank and a broker. These entities are also issued certificates by some certification authority (CA) within this WPKI. ME utilize the USIM (Universal Subscriber Identity Module) to store mobile client's information such as IMSI (International Mobile Subscriber Identity) and WPKI components. ME is capable of verifying digital signatures to authenticate other entities, if necessary. We also deploy a middleware called the broker to help ME authenticate the merchant server such that attackers cannot impersonate this seller. Merchant servers can perform PKI operations for evidence generations.

A Mobile Agent, namely, is a type of software agent, with the feature of autonomy, social ability, learning, and most importantly, mobility. A Mobile Agent, namely, is a type of **software agent**, with the feature of autonomy, social ability, learning, and most importantly, mobility. It is a process that can transport its state from one environment to another, with its data intact, and be capable of performing appropriately in the new environment. Mobile agents decide when and where to move. Movement is often evolved fromRPC methods. Similarly, a mobile agent accomplishes a move through data duplication. When a mobile agent decides to move, it saves its own state, transports this saved state to the new host, and resumes execution from the saved state.

A mobile agent is a specific form of mobile code. However, in contrast to the Remote evaluation and Code on demandprogramming paradigms, mobile agents are active in that they can *choose* to migrate between computers at any time during their execution. This makes them a powerful tool for implementingdistributed applications in a computer network. An open multi-agent system is a system in which agents that are owned by a variety of stakeholders continuously enter and leave the system.

More specifically, a mobile agent is process that can transport its state from one environment to another, with its data intact, and be capable of performing appropriately in the new environment. Mobile agents decide when and where to move.

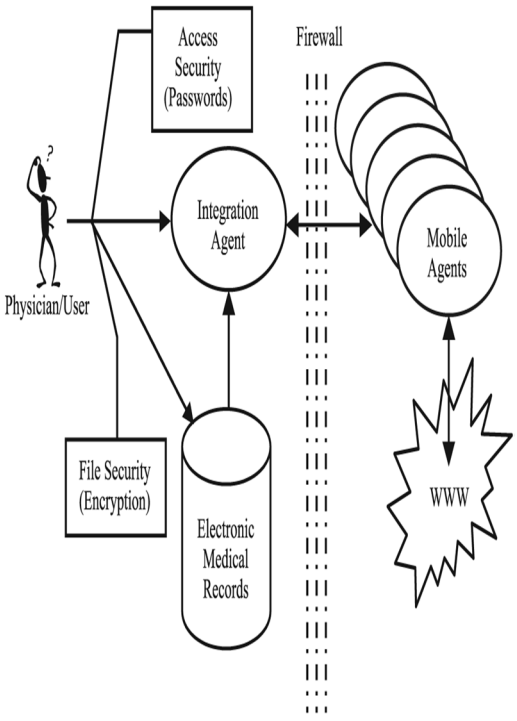

Figure. 1. Mobile Agent

Non-repudiation refers to a state of affairs where the purported maker of a statement will not be able to successfully challenge the validity of the statement or contract. The term is often seen in a legal setting wherein the authenticity of a signature is being challenged. In such an instance the authenticity is being "repudiated". The crypto logical meaning and application of non-repudiation shifts to mean:

- A service that provides **proof of the integrity** and **origin of data**.
- An authentication that with high assurance can be asserted to be genuine

Proof of data integrity is typically the easiest of these requirements to accomplish. A data hash, such as SHA2, is usually sufficient to establish that the likelihood of data being undetectably changed is extremely low. Even with this safeguard, it is still possible to tamper with data in transit, either through a man-in-the-middle attack or phishing. Due to this flaw, data integrity is best asserted when the recipient already possesses the necessary verification information.

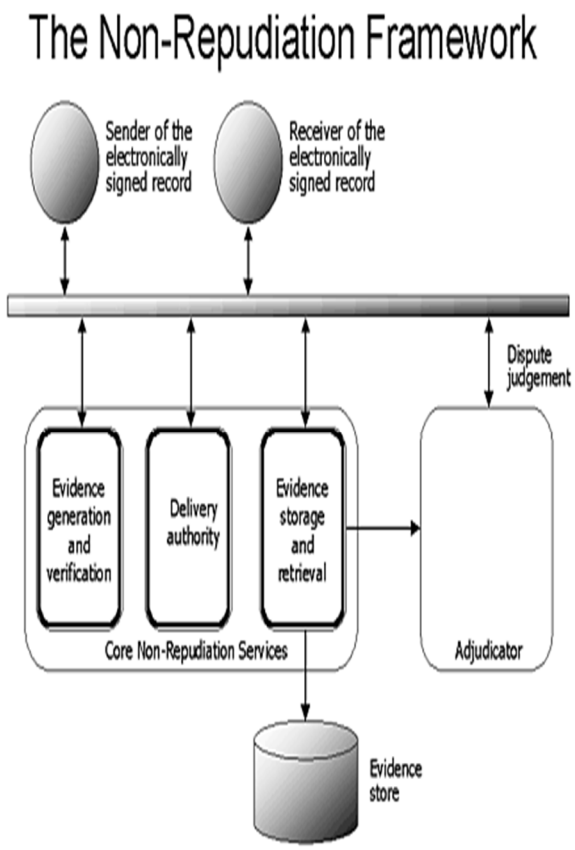

Figure.2 Non-Repudiation Frame Work

2. PRELIMINARY KNOWLEDGE

3G communication can be analyzed by the capability of the implementing cryptographic operation such as digital signature, symmetric key encryption/decryption, hash function and random number generation. According this investigation, we design a non-repudiation protocol adaptive to agent-based mobile digital right management systems.

A. Wireless Public Key Infrastructure

Wireless Public key infrastructure is used as cryptographic mechanism for non-repudiation protocol. It consists of two parts one is the operation and another is entity. WPKI entities must contain at least two public and private key pairs for encryption and decryption for the signature generation and for the verification respectively. The public key will be stored in some certificate field such as Certificate Authority will issue (subscriber) certificates and server certificates to buyers and varied servers, respectively. Where users may issue proxy certificates to their mobile agents for transaction delegations. The digital signature of a message is generated by using the private key of message owner and some hash function.

B. Trusted Third Party

Trusted third party (TTP). The trusted third party here is a notary server which simply generates necessary evidences for buyers and sellers. TTP needs to perform WPKI operations according to the non-repudiation protocol. Therefore TTP needs to access CA's repository to retrieve necessary certificates of the user's (rights issuers') and verify digital signatures. TTP needs to store the broker's public-key certificates and plays a role as the time stamp authority if necessary. For those generated Evidences, TTP will store these information in its public directory from which users and rights issuers may fetch evidences.

We focus on evidence generations of exchanging a right object between a mobile client and a rights issuer. These evidences are the foundation of the mobile DRM system. Time evidence of sending and receiving a right object is crucial in mobile DRM. It could be achieved by adding some time stamps to evidences. This improvement needs only TTP plays the role of time stamping authority while users and rights issuers just define their intended time spans. A non-repudiation protocol is fair if it can ensure that at the end of a protocol execution, none or both of the two entities, the sender and the receiver, can retrieve all the evidences it expects. Fairness guarantees that neither sender nor receiver can gain advantage over the other.

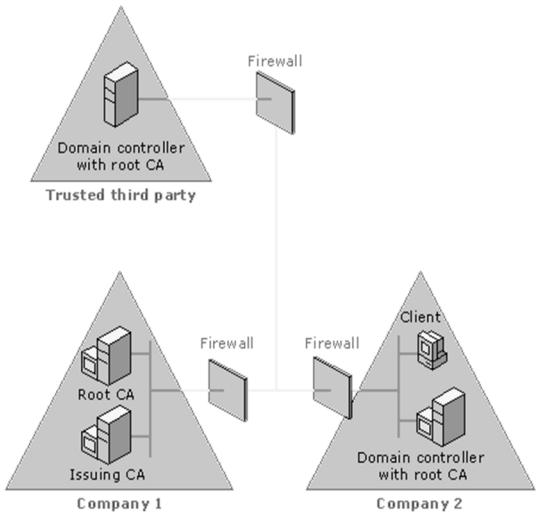

Figure.3.Trusted Third Party

The user (U) access a web server to find what right objects (RO) should purchase in order to access a protected content. Then this user contacts RI through the mobile network operator, sending the request of right (RORequest). RI will send response of right (ROResponse) to TTP, which will wait for U to take it, if the payment information is verified. Now we design a fair non-repudiation protocol suitable for agent-based

mobile DRM, this protocol also relies on the trust that broker will act according to the HRLs.

Trust is more a social issue than a technical one. We may assume reasonably that mobile operators or some service providers provide brokers which are completely trusted by mobile subscribers. The purpose of this non-repudiation protocol is to transmit encrypted payment information M and obtain non-repudiation evidences for U and RI.

C. Proxy Certificate

A proxy consists of a new certificate and a private key. The key pair that is used for the proxy, i.e. the public key embedded in the certificate and the private key, may either be regenerated for each proxy or obtained by other means. The new certificate contains the owner's identity, modified slightly to indicate that it is a proxy. The new certificate is signed by the owner, rather than a CA. (See diagram below.) The certificate also includes a time notation after which the proxy should no longer be accepted by others. Proxies have limited lifetimes.

The proxy's private key must be kept secure, but because the proxy isn't valid for very long, it doesn't have to kept quite as secure as the owner's private key. It is thus possible to store the proxy's private key in a local storage system without being encrypted, as long as the permissions on the file prevent anyone else from looking at them easily. Once a proxy is created and stored, the user can use the proxy certificate and private key for mutual authentication without entering a password.

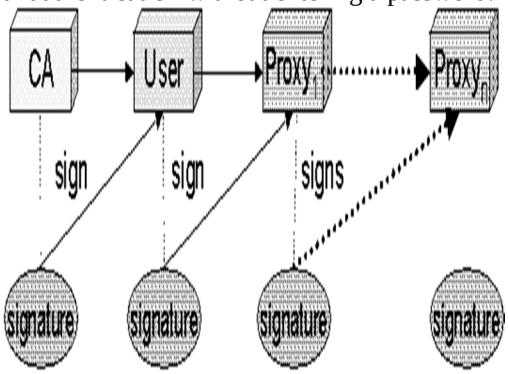

Figure.4. Proxy Certificate

When proxies are used, the mutual authentication process differs slightly. The remote party receives not only the proxy's certificate (signed by the owner), but also the owner's certificate. During mutual authentication, the owner's public key (obtained from her certificate) is used to validate the signature on the proxy certificate. The CA's public key is then used to validate the signature on the owner's certificate. This establishes a chain of trust from the CA to the proxy through the owner.

3. PROTOCOLS

When a message is received, the recipient may need to verify that the message has not been altered in transit. Furthermore, the recipient may wish to be certain of the originator's identity. Multi-hop wireless network is a wireless communication network without centralized control mechanism. Network nodes organize themselves automatically, and help other nodes relay data packets if they are not within the communication range. Study of protocol designed for such networks has been very challenging. Hence, simulations are always utilized to obtain the desired. OPNET and *ns*2 are the two most popular simulators used in network simulation, and *ns*2 as a open source software has attracted more attention in recent years. However, the implementations of routing protocol in *ns*2 are non-trivial. In this paper, we conduct a case study of implementing a routing protocol is *ns*2. The widely used routing protocol AODV is selected to demonstrate the implementation procedures. The methods of collecting and analyzing simulation results are also reviewed and discussed.

AODV discovers routes on an on-demand basis using a similar route discovery process as in DSR. AODV uses traditional routing tables, one entry per destination for maintaining routing information. DSR on the other hand maintains multiple route cache entries for each destination. To propagate route reply back to the source and to route data packets to the destination, AODV relies on routing table entries. Sequence numbers at each destination determines freshness of routing information and prevents routing loops. Routing packets carry the sequence numbers. The maintenance of timer-based states in each node for utilization of individual route entries is an important feature of AODV protocol. Sets of predecessor nodes are maintained for each routing table entry, which indicates the set of neighboring nodes. Route Error packets are used to notify these nodes when the next -hop link breaks. All the routes using the broken link are erased when the route error packets are sending to its own set of predecessors.

Route Error packets in AODV are intended to inform all sources using a link when a failure occurs. In AODV, Route Error propagation is visualized as a tree structure where the root is the node at the point of failure and all sources using the failed link as leaves. An optimizing technique in AODV to control Route Request flood in the route discovery process is to use an expanding ring search to discover routes to unknown destination. DSR with the influence of source routing and promiscuous listening of data packet transmissions has access to a significantly greater amount of routing information than AODV. AODV can gather only limited

amount of routing information. DSR uses route caching aggressively by replying to all requests reaching a destination from a single request cycle. In AODV, the destination replies only once to the request arrive first. The rest of the requests are ignored. AODV when faced with the choice of stale routes would choose the fresher one. The entry in the routing table if not used recently gets expired

4. CONCLUSIONS

We proposed a fair non-repudiation protocol based on mobile agents and proxy certificates. An evidence of mobile transaction is generated by WPKI mechanism such that user and rights issuer cannot repudiate sending and receiving payment information, respectively. One challenge of non-repudiation protocols is to avoid any entity to cheat and gain advantage over the other. Mobile DRMs need **"time information"** included in evidences for dispute resolutions. Users generate mobile agents which carry encrypted payment information to RIs. Mobile agent carries proxy certificate issued by its owner. The advantage of this agent-based protocol is to provide a ***convenient way for mobile clients*** to reach non-repudiation for mobile DRMs. According to binding mechanism of the proxy certificate and its corresponding subscriber certificate, mobile agent and its owner cannot repudiate their relationship; this is crucial for agent-based mobile DRM systems. Reducing The TTP Involvement, TTP provides directory services accessible to the public. For the non-repudiation protocols introduced, TTP only deal with ''keys'' rather than purchase order, that is, TTP does not know any information of this order. Therefore the communications overheads between parties and TTP are reduced, and the user's purchasing privacy is also guaranteed.

REFERENCES

[1] Bamasak, O., Zhang, N. (2005). A distributed reputation management scheme for mobile agent-based e-commerce applications. In IEEE International Conference on e-Technology, e-Commerce and e-Service.

[2] Borrell, J., Robles, S., Serra, J., Riera, A. (1999). Securing the itinerary of mobile agents through a non-repudiation protocol, In IEEE 33rd Annual 1999 International Carnahan Conference on Security Technology.

[3] Esparza, O., Munoz, J., Soriano, M., Forne, J. (2003). Host revocation authority: a wayof protecting mobile agents from malicious hosts, ICWE 2003, LNCS 2722, pp.289–292.

[4] Grossklags, J., & Schmidt, C. (2006). Software agents and market (in) efficiency: Ahuman trader experiment. IEEE Transactions on Systems, Man and Cybernetics Part C, 36(1), 1–13.

[5] Hamdi, M. S. (2006). MASACAD: A multiagent-based approach to information customization. IEEE Intelligent System, 21(1), 60–67.

[6] ITU-T. (1996). Recommendation, X.813: information technology-open systems interconnection- security frameworks in open systems. Non-repudiation framework.

[7] Lee, W.-B., &Yeh, C.-K. (2005). A new delegation-based authentication protocol for use in portable communication systems. IEEE Transactions on Wireless Communications, 4(1).

[8] Li, B., &Luo, J. (2004). On timeliness of a fair on-repudiation protocol. InfoSecu'04, 14-16, 99–106.

[9] Liew, C.-C., Ng, W.-K., Lim, E.-P., Tan, B.-S., Ong, K.-L. (1999). Non-repudiation in an agent-based electronic commerce system, DEXW Workshop.

[10] M'Raihi, D., & Yung, M. (2001). E-commerce applications of smart cards. Computer Networks, 36, 453–472.

[11] Onieva, J., Lopez, J., Roman, R., Zhou, J., &Gritzalis, S. (2007). Integration of non-repudiation services in mobile DRM scenarios. Telecommunication Systems, 35, 161–1765.

[12] Tseng, Y.-M., Yang, C.-C., & Su, J.-H. (2004). Authentication and billing protocols for the integration of WLAN and 3G networks. Wireless Personal Communications, 29, 351–366.

[13] Wang, F.-Y. (2005). Agent-based control for networked traffic management systems. IEEE Intelligent System, 20(5), 92–96.