Enhanced Security Model of E-Cash system in Wireless Mesh Networks

Asifa Begum.S

PG Scholor
Department of Computer Science and Engineering, Nehru Institute of Technology, Coimbtaore, India
asif.yuga@gmail.com

***Abstract* - — In today's fast moving world, everything can be done by electronically for the purpose of providing fast and comfortable communication in this case providing trust worthy environment is a challenging task. Security in all aspects has become a major concern. Anonymity allows user to enjoy network services without any difficulties of accessing procedure but it provides the gateway of hacker's introduction. In this paper, an Attack-Resilient Security Architecture (ARSA) proposed for WMNs to ensure unconditional anonymity for honest users and traceability of misbehaving users for network authorities in WMNs. This also strives to resolve the conflicts between the anonymity and traceability objectives in addition to guaranteeing fundamental security requirements including authentication, confidentiality, data integrity, and non-repudiation. By considering an e-cash systems in which conditional anonymity is implemented, such that misbehaving entities in the network remain traceable. Hence this kind of anonymity provides protection for honest users to enjoy network services without being traced. The main purpose of this security model is to enable successful transactions among users. Here we are providing a high level of security for the trusted users by allowing them to undergo transaction only during an allotted time interval. Also trace out the misbehaviour at the time of cheating itself by using trusted monitors in a network. The highlight of this scheme is instead of using a database, an object file is used to ensure a high level of security. This indeed stresses on the fact that is mainly trying to achieve security in all aspects including database too.**

Keywords: e-cash,Wireless Mesh Network(WMN), anonymity, traceability,security, misbehaviour, users, transaction,trust monitor.

I.INTRODUCTION

Wireless Mesh Network (WMN) is a promising technology and is in an ever increasing demand. Wireless security has been the hot topic in the literature for various network technologies such as cellular networks, wireless local area networks (WLANs), wireless sensor networks, mobile ad hoc networks (MANETs) and thereby providing security is damn important.

Anonymity provides protection for users to comfortable network services without being traced. Anonymity is by large the most used technological word which ensures the privacy of the user information to be maintained by hiding the identity of the user. In many security related applications, anonymity is by large the most important aspect that is achieved.

Traceability is the most important aspect that needs to be implemented in almost all the security related applications. The word traceability actually implies that the identity of the user is revealed in the case of any kind of hacking taking place. On the other hand it has to be ensured that that the conflict between traceability and anonymity is resolved. Consider a bank application which is based on E-cash systems ,in a bank a user may be a seller/buyer. The banker is the gateway for performing a successful interaction between the users. The banker possesses the main responsibility of tracing the misbehaving entity. Thereby all the actions performed by the user gets traced on the banker side. This on the other hand, enables to reveal the identity of the misbehaving entity.

Key generation takes place in the bank and is accessed by all the users only when there is a need for the process of transaction. The ticket issuance concept is brought into existence by the provision of a secured amount of time whenever the user wants to carry out a transaction.

II.RELATED WORK

Wei.K. et. al Suggests that A numerous anonymous payment systems have been proposed to hide user identities during transactions, mostly by using blind signatures or public key cryptography. A common characteristic shared by all the payment schemes is that every transaction goes through a central authority, which we refer to in general as the broker. In Who Pay, a peer-to-peer payment system that provides anonymity, represents coins with public keys; for scalability, we distribute coin transfer load across all peers, rather than rely on a central entity such as the broker. This basic version of WhoPay is secure and scalable such as PPay.

S. Zhu. et. al (2009) suggests A fundamental issue that must be addressed when using key management protocols based on symmetric shared keys is the mechanisms used for establishing the shared keys. An important design consideration for security protocols based on symmetric keys is the degree of key sharing between the nodes in the system. At one extreme, we can have a network-wide keys that are used for encrypting data and for authentication. This paper assumes however that the immediate

neighboring nodes of any sensor node will not be known in advance LEAP is designed to support secure communications in sensor networks; therefore, it provides the basic security services such as confidentiality and authentication.

Gianni A.et.al suggests that optimal relay node placement for throughput enhancement in wireless sensor networks, the main objective is to define relay node location for increasing the network performances by means of delivery ratio, end to end delay to provide connectivity in a partially disconnected area. It uses a dynamic routing protocol for the wireless network communication which is dynamically adapted to the changing conditions.

M. Raya. et. al suggests It allows vehicles communicate with each other and with roadside infrastructure; in this way, vehicles will dramatically increase their awareness of their environment, thereby increasing safety and optimizing traffic. The communicating nodes in VANETs are either vehicles or base stations. An advantage of VANETs over "usual" ad hoc networks is that vehicles provide substantial computational and power resources, especially taking into account Moore's law. This paper provides a general classification of attacks substantiated by a list of attacks that we have identified so far. It is not possible without defining several performance related aspects, such as the power of on-board processors. But even analytically, the major performance characteristics of each technique can be seen and make a conclusion that favors digital signatures.

III.SYSTEM MODEL

There are several security approaches are introduced , most of the existing mechanism focuses on providing security in wireless communication.it makes the architecture of security model in a difficult way, traceability is missing in case of cheating occurrence time itself. privacy of user is need to be maintained for user friendly services of network users but it results the conflicts of achieving traceability.this paper mainly deals with the E-cash systems. Increased number of E-cash application available in wireless networks. Net banking system plays a vital role in transcaction using e-cash. The workflow of enhanced security architecture of banking system is shown in figure1.1.

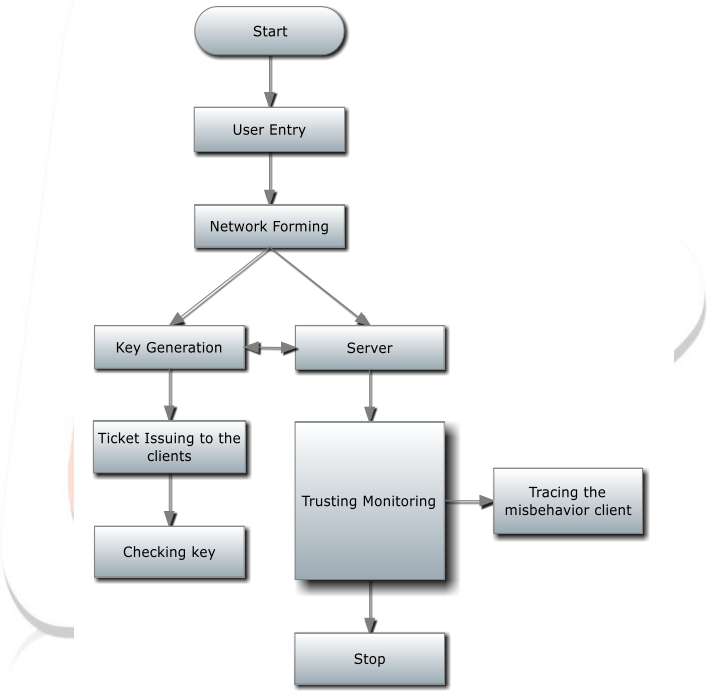

Figure 1.1 system model of banking system

This paper is based on an e - cash system where the transaction takes place between users (buyer and seller) based on the product which is purchased. In the first note, the users are permitted to enter into the network and this is enabled by providing the user with the facility of creating an account. This process of account creation is done by the central authority i.e., The banker.

Once accounts are created, the key is generated by the banker, which is essential for the commencement of the transaction. In order to access the key generated by the bank the user needs to enter in the IP address of the bank. Only when this is done the transaction between the users can actually commence. This ensures the level of security enhancement.

For the buyer to buy the product, he/she should possess sufficient amount. This can be possible by withdrawing amounts from his/her account. Once this is done, the buyer needs to enter in the IP address of the seller to perform the transaction. This is possible only when the server on the seller side is in the server start mode. If the seller is in server shutdown mode the transaction process will not be allowed to proceed further. The denominations of the notes available to the user can be checked out or cross checked by viewing the notes availability option.

If the transaction takes place successfully, the seller is providing the provision of depositing the amount in his/her account. The entire process is monitored by the banker. If at all a password mismatch occurs at any stage of the process it gets monitored on the banker side. This ensures a high level of security at each and every stage of the transaction process.

3.1 *Network Formation*

The banking sector is a resource of transaction process in the world of communication. Multiple users can create their own account from a remote place through a wireless network. By means of providing secure transaction to users first step is to form a network which provides the easiest way of transaction among the various users available in wireless mesh network.

3.2 Key Generation

The banker is the entity which is used to connect the multiple buyer and multiple seller in a network. The connection is made by generating keys and sharing between the involved entities (buyer and seller). The key is generated by using RSA algorithm. Whenever a user request the banker for the process of the transaction, the key is generated by using the IP address of user requests.

Algorithm for Key generation

1. Generate two large random primes, *p* and *q*, of approximately equal size such that their product n = pq is of the required bit length.
2. Compute n = pq & φ = (p-1) (q-1).
3. Choose an integer *e*, 1 < e < φ , such that
   i. gcd (e, φ) = 1.
4. Compute the secret exponent *d*, 1 < d < φ, such that
   i. e*d ≡ 1 (mod phi).
5. The public key is (n, e) and the private key (d, p, q). The values d, p, q and φ are always kept secret to ensure security.

After the key generation, public key is shared for the interaction between buyer and seller for the purpose of ensuring secure transaction**.**

3.3 Server Availability

Server availability is another important aspect related to E-cash transaction. It incurs that whenever the buyer buys a product from the seller it is obvious that he/she has to pay to the seller. The server is not in the server start mode always. The server should either be in the server start mode, or server shutdown mode. This insists that the buyer can repay to the system only when the seller is in the server start mode. This ensures that the money is paid to the right user and the misplace of the money is avoided. This process takes place only when the server on the seller side is in the server start mode. If this is not the case the buyer is not allowed to pay to the seller thus enhancing the security.

3.4 Ticket Issuance

Ticketing system is used for ensuring security features to the users who are involved in the transaction as well as trace out the misbehavior actions in the network. The users are permitted to avail the services only for a particular amount of time with the help of the two processes namely SERVER START and SERVER SHUTDOWN. Each Ticket 'c' has 3 values which is defined as (Val; exp; mis), where Val, exp and mis denote the ticket value, expiry date/time, and the client's misbehavior level, respectively. Ticket reuse is also a kind of misbehaviour activity, this action is noted by the trust monitor and reject the transaction if it resued or time expired.

3.5 Tracing and Anonymity

The main idea behind our work is to trace the entire process and to prevent any misbehavior. The central administrator, banker is provided the provision of tracing the action right from the process of account creation till the end of a transaction between the users. In some cases where a cheat occurs, it get monitored on the banker side. With this kind of provision provided to the banker a high level of security is ensured to the user/client.

In order to achieve anonymity user details are available only in the bank, which is a trusted system. Since banker monitors every action performed by the users it is easy to trace out. Untrusted users are blocked at the initial stage itself in case any password mismatch. In such case the account id is displayed in the bank. Interior attacks cannot be achieved by the misbehavior due to the provision of a secured session by the server.

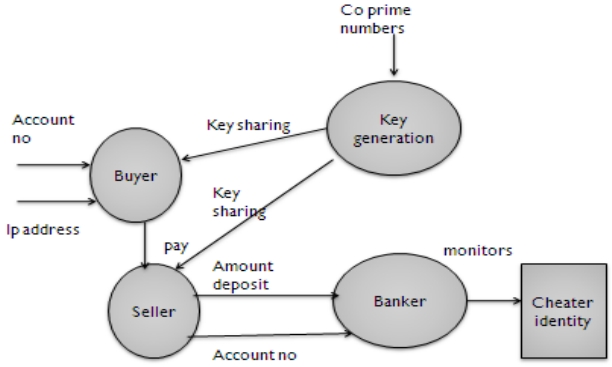

Figure 1.2: traceability in banking system

3.6 Performance Evaluation

The performance of this security approach in the banking system is validated in terms of the availability of notes which is also a means of security provision. Supposing a transaction takes place between a buyer and a seller, the buyer deposits the notes on the seller side. One of the validation processes that are performed here is that only when the seller is in the SERVER START mode the notes can be deposited by the seller. Hence the misplacing of the notes is avoided. On the other hand, when the seller receives the notes and he/she wants to deposit it back to the bank, the nomination of the notes needs to be matched, only then the depositing is allowed. This also ensures validation of the process performed.

IV.CONCLUSION

An initiative approach of security for the transactions has been provided. Here I propose a security architecture that mainly resolves the conflicting security requirements of unconditional anonymity for honest users, and traceability of misbehaving users. This Scheme is mainly based on the e-cash system, thrives to provide the highest level of security to the trusted user. On the other hand the misbehaving user is not allowed to involve in further transactions. With the help of the key generation and ticketing concepts, the proposed architecture is demonstrated to achieve desired security objectives and efficiency. One of the highlights of the approacht is the usage of object files which adds on for enriching the security justifying the objective of this scheme. Thus the concept can be enhanced even better to produce the benchmark of results.

REFERENCES

[1] J. Sun, C. Zhang, and Y. Fang, "A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks," Proc. IEEE INFOCOM, pp. 1687-1695, Apr. 2008.
[2] N.B. Salem and J-P. Hubaux, "Securing Wireless Mesh Networks," IEEE Wireless Comm., Vol. 13, no. 2, pp. 50-55, Apr. 2006.
[3] A. Juels, M. Luby, and R. Ostrovsky, "Security of Blind Digital Signatures," Advances in Cryptology—Crypto '97, pp. 150-164, Springer-Verlag, 1997.
[4] Y. Zhang, W. Liu, W. Lou, and Y. Fang, "Securing Mobile Ad Hoc Networks with Certificateless Public Keys," IEEE Trans. Dependable and Secure Computing, vol. 3, no. 4, pp. 386-399, Oct. 2006.
[5] I.F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," Computer Networks, vol. 47, no. 4, pp. 445-487, March 2005.
[6] [S. Brands, "Untraceable Off-Line Cash in Wallets with Observers,"Proc. 13th Ann. Int'l Cryptology Conf. Advances in cryptology (CRYPTO '93), pp. 302-318, Aug. 1993.
[7] A.R. Beresford and F. Stajano, "Location Privacy in Pervasive Computing,"IEEE Pervasive Computing, vol. 2, no. 1, pp. 46-55, Jan.-Mar. 2003.
[8] [22] J. Sun, C. Zhang, and Y. Fang, "A Security Architecture Achieving Anonymity and Traceability in Wireless Mesh Networks,"Proc. IEEE INFOCOM, pp. 1687-1695, Apr. 2008.
[9] D. Boneh and M. Franklin, "Identity-Based Encryption from the Weil Pairings,"Advances in Cryptology-Asiacrypt 2001, pp. 514-532, Springer-Verlag, 2001.
[10] X. Chen, F. Zhang, and S. Liu, "ID-Based Restrictive Partially Blind Signatures and Applications," J. Systems and Software,vol. 80, no. 2, pp. 164-171, Feb. 2007.
[11] R. Dutta, R. Barua, and P. Sarkar,Pairing-Based Cryptography: A Survey, Cryptology ePrint Archive, Report 2004/064, http://eprint.iacr.org/2004/064.pdf, 2004.
[12] S.D. Galbraith, "Pairings,"Advances in Elliptic Curve Cryptography,I.F. Blake, G. Seroussi, and N.P. Smart, eds., pp. 183-213, chapter 9,Cambridge Univ. Press, 2005.
[13] H.W. Lim, "On the Application of Identity-Based Cryptography inGrid Security," PhD thesis, Univ. of London, 2006.
[14] X. Wu and N. Li, "Achieving Privacy in Mesh Networks,"Proc.Fourth ACM Workshop Security of Ad Hoc and Sensor Networks (SASN '06), pp. 13-22, Oct. 2006.
[15] R. Dingledine, "Tor: An Anonymous Internet Communication System," Proc. Workshop Vanishing Anonymity, the 15th Conf.Computers, Freedom, and Privacy,Apr. 2005.