IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

A Novel Approach for Cryptography Architecture achieving the secure anonymity in mobile ad-hoc networks

Mr.S. Prasanth[1]

Assistant Professor / CSE,
Unnamalai Institute of Technology, Kovilpatti,
Tamilnadu, India.

Mrs.C.Ajitha

Assistant Professor/CSE
Unnamalai Institute of Technology,Kovilpatti
Tamil nadu ,India

Abstract Anonymity and traceability is more important for e-cash payment system and wireless mesh network. An anonymity network enables users to access the Web while their identity on the Internet is blocked. Anonymity networks prevent traffic analysis and network observation or at least make it more difficult. WMN domains are managed by different operators. Therefore the misbehavior recognition and tracing is more complicated. So we propose a ticket based security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users in WMNs. This architecture 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.

Keywords: Anonymity, Traceability, Pseudonym, Misbehavior, Revocation, WMN

INTRODUCTION

Wireless Mesh Network (WMN) represent a good solution to provide wireless internet connectivity in a sizeable geographic area. It is a communication network made up of radio nodes organized in a Mesh topology. A mesh network is consistent and offers idleness. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. This new and promising paradigm allows network deployment at a much lower cost. The requirement of anonymity is to unlink a user's identity to his or her specific activities. It is also required to hide the location information of a user to prevent movement tracing in mobile networks and VANET'S. Traceability is highly desirable in e-cash system where it is used for detecting and tracing double spenders. In this system, we are motivated by resolving the above security conflicts, namely anonymity and traceability, in the Emerging WMN communication systems. Our system uses the blind signature technique to achieve the anonymity of unlinking user identities from activities, as well as the traceability of misbehaving users. Furthermore, the pseudonym technique is used to extract user location information unexposed.

I. RELATED WORK

L.Zhou and Z.J.Haas [4] proposed Ad-hoc networks which is a new wireless networking paradigm for mobile host. Ad-hoc networks do not rely on any fixed infrastructure. Instead, hosts rely on each other to keep the network connected. This system is proposed to handle a public key infrastructure because of its superiority in distributing keys and in achieving integrity and non-repudiation.

Jinyuan Son, Chi Zhang, Yanchao Zhang and Yuguang Fang [9] proposed security architecture to ensure unconditional anonymity for honest users and traceability of misbehaving users for networks authorities in WMNs. Anonymity provides protection for users to enjoy network services without being traced.

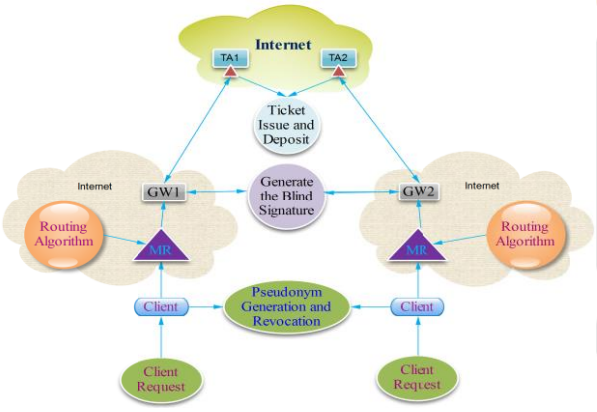
S.M.M.Rahman, A.Inomata, T.Okamoto, M.Mambo and E.Okamoto [7] proposed a system to handle pairing based cryptography to generate pseudo IDs of the nodes. RIOMO reduces pseudo IDs maintenance costs. Only trust-worthy nodes are allowed to take part in routing to discover a route. RIOMO provides different anonymous properties such as identity privacy, location privacy, route anonymity, and robustness against several attacks.

A.Juels, M.Luby, and R.Ostrovsky [8] proposed a system to handle the notion of blind digital signatures as a key tool for constructing various anonymous electronic cash instruments. By using this system the bank cannot trace where a user spends her electronic currency. The security of the signature scheme should guarantee that it is difficult for the user to forge a signature of any additional document.

NEED OF THE STUDY.

ID-based cryptography (IBC) allows the public key of an entity to be derived from its public identity information such as name and e-mail address, which avoids the use of certificates for the public key verification in the conventi- onal public key infrastructure (PKI).In our system we pro- pose Hierarchical ID-based encryption (HIDE) which all- ows a root PKG to distribute the workload by delegating private key generation and identity authentication to lower-level PKGs. In a HIDE scheme, a root PKG need only to generate private keys for domain-level PKGs,

who in turn generates private keys for users in their domains in the next level.



II. TICKET BASED ARCHITECTURE

A. Client and Trusted Node Deployments

The TA is trusted within the WMN domain. There is no direct trust relationship between the client and the gateway/mesh router. We are using standard IBC for authentication and secure communications both at the backbone and during network access inside a trust domain (i.e., intra domain). We further assume the existence of pre-shared keys and secure communication channels between entities (TAs, gateways, mesh routers) at the backbone and will solely consider the authentication and key establishment during the network access of the clients. The client presents his ID upon registration at the TA, which assigns a private key associated with the client's ID.

B. Ticket Issuance and Deposit Process

Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets are depleted. The client needs to expose his real ID to the TA in order to obtain a ticket since the TA has to ensure the authenticity of this client. Moreover, the TA should be unable to link the ticket it issued to the clients' real identities. The client thus employs some blinding technique to transform the ticket to be un-linkable to a specific execution of the ticket generation algorithm (the core of ticket issuance protocol), while maintaining the verifiability of the ticket. The ticket generation algorithm, which can be any restrictive partially blind signature scheme, takes as input the client's and TA's secret numbers, the common agreement c, and some public parameters, and generates a valid ticket = {TN;W; C; (U'; V';X';)} at the output.

C. Generate Pseudonym and Revocation Process

The pseudonym is used to replace the real ID in the authentication, which is necessary for both anonymous network access and location privacy. In the intra-domain authentication in our system, the client generates his own pseudonym by selecting a secret number $2 and computing the pseudonym PS_{CL} {H1, ID_{CL}, and P} [7]. The self-generation method vastly reduces the communication overhead in the system. The client is able to frequently update his/her pseudonyms to enhance anonymity by using this inexpensive method. The TA will also be able to derive the real identity corresponding to the assigned pseudonyms, which destroys the anonymity for honest clients.

D. Blind Signature Generation

A blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer [8]. The first restrictive blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information. Partial blind signature schemes [10] allows the resulting signature to convey publicly visible information on common agreements between the signer and the signee.

E. Fraud Detection and Ticket Revocation Process

Ticket reuse generally results from the client's inability to obtain tickets from the TA when network access is desired, primarily due to the client's past misbehavior, which causes the TA to constrain his ticket requests. Multiple-deposit can also be termed client coalition, which is beneficial when the coalescing parties are unauthorized users or clients with misbehavior history having difficulty in acquiring tickets from the TA. This approach will eliminate the multiple deposit fraud but requires the deployment of secure modules. In the following discussion, we will still consider multiple deposit as a possible type of fraud.

These two types of fraud share a common feature, that is, a same ticket (depleted or valid) is deposited more than once such that our one-time deposit rule is violated.

Ticket Revocation is necessary when a client is compromised, and thus, all his secrets are disclosed to the adversary. Therefore, the compromised client needs to be able to revoke the ticket and prevent the adversary from acquiring benefits. The ticket revocation protocol consists of two cases.

Revocation of new tickets: the client may store a number of unused tickets, as mentioned previously. When revoking these tickets that have not been deposited, the client sends PS_{CL},TN,t_{10}, in the revocation request to any SIG T_{CL} ~(TN)||t_{10} encountered gateway. This gateway authenticates the client using PS_{CL} and records the ticket serial number TN as revoked.

Revocation of deposited tickets: the client simply sends PS_{CL}, ID_{DGW}, t_{11}, SIG, in the revocation request to the DGW. The DGW authenticates the client and marks the associated ticket revoked.

F. Accessing the network from foreign domains

The access services the visiting (foreign) trust domain provided the ticket-based security architecture can take place in two ways including the following:

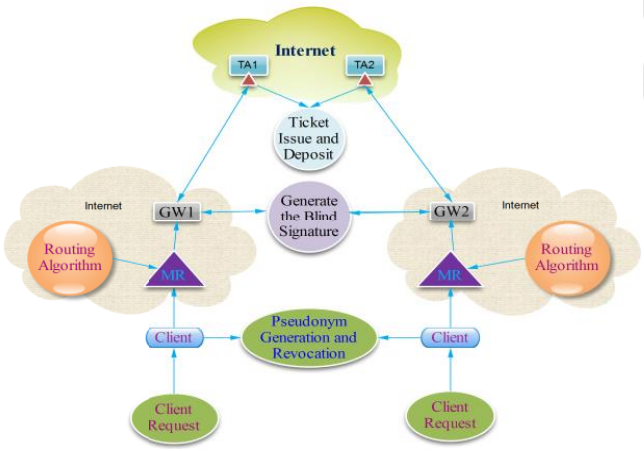
- A foreign mesh router MR (or foreign access point) forwards the client's new ticket request to the home domain when there is no available ticket for accessing the network from the foreign domain.
- MR (or an access point) forwards the client's ticket deposit request to the home domain when the client owns available new tickets issued by the home TA.

It is recommended that the client registers with the foreign TA to become an affiliated user of the foreign domain. Consequently, all the network access-related operations including ticket issuance, deposit, revocation, and fraud detection will follow the same procedures as in the home domain case, which greatly reduces the communication overhead in the system.

G. Inter-Domain Authentication from Mesh Router

Inter-domain authentication is more important for wireless peer-to-peer authentication networks. The mesh router generates and initialize the Defense ID for each client. The client first generates the Resistance ID and gives the resistance ID to mesh router. The mesh router receives that ID and registers the client resistance ID and send to home domain mesh routers. The mesh router sends the defense ID to client.

ID-based cryptography (IBC) allows the public key of an entity to be derived from its public identity information such as name and e-mail address, which avoids the use of certificates for the public key verification in the conventi- onal public key infrastructure (PKI).In our system we pro- pose Hierarchical ID-based encryption (HIDE) which all- ows a root PKG to distribute the workload by delegating private key generation and identity authentication to lower-level PKGs. In a HIDE scheme, a root PKG need only to generate private keys for domain-level PKGs,
who in turn generates private keys for users in their domains in the next level.



III. TICKET BASED ARCHITECTURE

A. Client and Trusted Node Deployments

The TA is trusted within the WMN domain. There is no direct trust relationship between the client and the gateway/mesh router. We are using standard IBC for authentication and secure communications both at the backbone and during network access inside a trust domain (i.e., intra domain). We further assume the existence of pre-shared keys and secure communication channels between entities (TAs, gateways, mesh routers) at the backbone and will solely consider the authentication and key establishment during the network access of the clients. The client presents his ID upon registration at the TA, which assigns a private key associated with the client's ID.

B. Ticket Issuance and Deposit Process

Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets are depleted. The client needs to expose his real ID to the TA in order to obtain a ticket since the TA has to ensure the authenticity of this client. Moreover, the TA should be unable to link the ticket it issued to the clients' real identities. The client thus employs some blinding technique to transform the ticket to be un-linkable to a specific execution of the ticket generation algorithm (the core of ticket issuance protocol), while maintaining the verifiability of the ticket. The ticket generation algorithm, which can be any restrictive partially blind signature scheme, takes as input the client's and TA's secret numbers, the common agreement c, and some public parameters, and generates a valid ticket = {TN;W; C; (U'; V';X';)} at the output.

C. Generate Pseudonym and Revocation Process

The pseudonym is used to replace the real ID in the authentication, which is necessary for both anonymous network access and location privacy. In the intra-domain authentication in our system, the client generates his own pseudonym by selecting a secret number $2 and computing the pseudonym PS_{CL} {H1, ID_{CL}, and P} [7]. The self-generation method vastly reduces the communication overhead in the system. The client is able to frequently update his/her pseudonyms to enhance anonymity by using this inexpensive method. The TA will also be able to derive the real identity corresponding to the assigned pseudonyms, which destroys the anonymity for honest clients.

D. Blind Signature Generation

A blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer [8]. The first restrictive blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information. Partial blind signature schemes [10] allows the resulting signature to convey publicly visible information on common agreements between the signer and the signee.

E. Fraud Detection and Ticket Revocation Process

Ticket reuse generally results from the client's inability to obtain tickets from the TA when network access is desired, primarily due to the client's past misbehavior, which causes the TA to constrain his ticket requests. Multiple-deposit can also be termed client coalition, which is beneficial when the coalescing parties are unauthorized users or clients with misbehavior history having difficulty in acquiring tickets from the TA. This approach will eliminate the multiple deposit fraud but requires the deployment of secure modules. In the following discussion, we will still consider multiple deposit as a possible type of fraud.

These two types of fraud share a common feature, that is, a same ticket (depleted or valid) is deposited more than once such that our one-time deposit rule is violated.

Ticket Revocation is necessary when a client is compromised, and thus, all his secrets are disclosed to the adversary. Therefore, the compromised client needs to be able to revoke the ticket and prevent the adversary from acquiring benefits. The ticket revocation protocol consists of two cases.

Revocation of new tickets: the client may store a number of unused tickets, as mentioned previously. When revoking these tickets that have not been deposited, the client sends PS_{CL},TN,t_{10}, in the revocation request to any SIG T_{CL} ~(TN)||t_{10} encountered gateway. This gateway authenticates the client using PS_{CL} and records the ticket serial number TN as revoked.

Revocation of deposited tickets: the client simply sends PS_{CL}, ID_{DGW}, t_{11}, SIG, in the revocation request to the DGW. The DGW authenticates the client and marks the associated ticket revoked.

F. Accessing the network from foreign domains

The access services the visiting (foreign) trust domain provided the ticket-based security architecture can take place in two ways including the following:

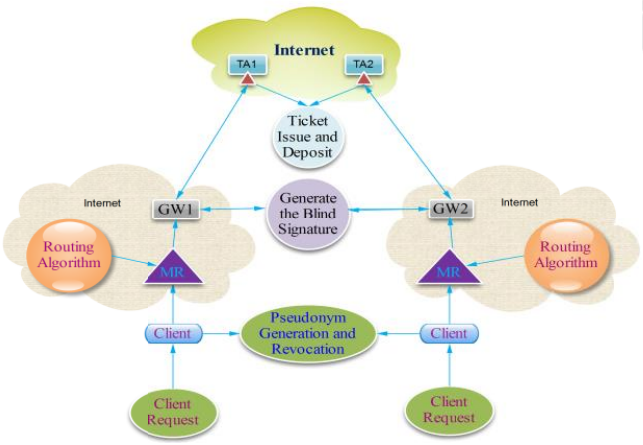
- A foreign mesh router MR (or foreign access point) forwards the client's new ticket request to the home domain when there is no available ticket for accessing the network from the foreign domain.
- MR (or an access point) forwards the client's ticket deposit request to the home domain when the client owns available new tickets issued by the home TA.

It is recommended that the client registers with the foreign TA to become an affiliated user of the foreign domain. Consequently, all the network access-related operations including ticket issuance, deposit, revocation, and fraud detection will follow the same procedures as in the home domain case, which greatly reduces the communication overhead in the system.

G. Inter-Domain Authentication from Mesh Router

Inter-domain authentication is more important for wireless peer-to-peer authentication networks. The mesh router generates and initialize the Defense ID for each client. The client first generates the Resistance ID and gives the resistance ID to mesh router. The mesh router receives that ID and registers the client resistance ID and send to home domain mesh routers. The mesh router sends the defense ID to client.

ID-based cryptography (IBC) allows the public key of an entity to be derived from its public identity information such as name and e-mail address, which avoids the use of certificates for the public key verification in the conventi- onal public key infrastructure (PKI).In our system we pro- pose Hierarchical ID-based encryption (HIDE) which all- ows a root PKG to distribute the workload by delegating private key generation and identity authentication to lower-level PKGs. In a HIDE scheme, a root PKG need only to generate private keys for domain-level PKGs,
who in turn generates private keys for users in their domains in the next level.



IV. TICKET BASED ARCHITECTURE

A. Client and Trusted Node Deployments

The TA is trusted within the WMN domain. There is no direct trust relationship between the client and the gateway/mesh router. We are using standard IBC for authentication and secure communications both at the backbone and during network access inside a trust domain (i.e., intra domain). We further assume the existence of pre-shared keys and secure communication channels between entities (TAs, gateways, mesh routers) at the backbone and will solely consider the authentication and key establishment during the network access of the clients. The client presents his ID upon registration at the TA, which assigns a private key associated with the client's ID.

B. Ticket Issuance and Deposit Process

Ticket issuance occurs when the client initially attempts to access the network or when all previously issued tickets are depleted. The client needs to expose his real ID to the TA in order to obtain a ticket since the TA has to ensure the authenticity of this client. Moreover, the TA should be unable to link the ticket it issued to the clients' real identities. The client thus employs some blinding technique to transform the ticket to be un-linkable to a specific execution of the ticket generation algorithm (the core of ticket issuance protocol), while maintaining the verifiability of the ticket. The ticket generation algorithm, which can be any restrictive partially blind signature scheme, takes as input the client's and TA's secret numbers, the common agreement c, and some public parameters, and generates a valid ticket = {TN;W; C; (U'; V';X';)} at the output.

C. Generate Pseudonym and Revocation Process

The pseudonym is used to replace the real ID in the authentication, which is necessary for both anonymous network access and location privacy. In the intra-domain authentication in our system, the client generates his own pseudonym by selecting a secret number $2 and computing the pseudonym PS_{CL} {H1, ID_{CL}, and P} [7]. The self-generation method vastly reduces the communication overhead in the system. The client is able to frequently update his/her pseudonyms to enhance anonymity by using this inexpensive method. The TA will also be able to derive the real identity corresponding to the assigned pseudonyms, which destroys the anonymity for honest clients.

D. Blind Signature Generation

A blind signature scheme allows a receiver to obtain a signature on a message such that both the message and the resulting signature remain unknown to the signer [8]. The first restrictive blind signature scheme, where the restrictiveness property is incorporated into the blind signature scheme such that the message being signed must contain encoded information. Partial blind signature schemes [10] allows the resulting signature to convey publicly visible information on common agreements between the signer and the signee.

E. Fraud Detection and Ticket Revocation Process

Ticket reuse generally results from the client's inability to obtain tickets from the TA when network access is desired, primarily due to the client's past misbehavior, which causes the TA to constrain his ticket requests. Multiple-deposit can also be termed client coalition, which is beneficial when the coalescing parties are unauthorized users or clients with misbehavior history having difficulty in acquiring tickets from the TA. This approach will eliminate the multiple deposit fraud but requires the deployment of secure modules. In the following discussion, we will still consider multiple deposit as a possible type of fraud.

These two types of fraud share a common feature, that is, a same ticket (depleted or valid) is deposited more than once such that our one-time deposit rule is violated.

Ticket Revocation is necessary when a client is compromised, and thus, all his secrets are disclosed to the adversary. Therefore, the compromised client needs to be able to revoke the ticket and prevent the adversary from acquiring benefits. The ticket revocation protocol consists of two cases.

Revocation of new tickets: the client may store a number of unused tickets, as mentioned previously. When revoking these tickets that have not been deposited, the client sends PS_{CL},TN,t_{10}, in the revocation request to any SIG T_{CL} ~(TN)||t_{10} encountered gateway. This gateway authenticates the client using PS_{CL} and records the ticket serial number TN as revoked.

Revocation of deposited tickets: the client simply sends PS_{CL}, ID_{DGW}, t_{11}, SIG, in the revocation request to the DGW. The DGW authenticates the client and marks the associated ticket revoked.

F. Accessing the network from foreign domains

The access services the visiting (foreign) trust domain provided the ticket-based security architecture can take place in two ways including the following:

- A foreign mesh router MR (or foreign access point) forwards the client's new ticket request to the home domain when there is no available ticket for accessing the network from the foreign domain.
- MR (or an access point) forwards the client's ticket deposit request to the home domain when the client owns available new tickets issued by the home TA.

It is recommended that the client registers with the foreign TA to become an affiliated user of the foreign domain. Consequently, all the network access-related operations including ticket issuance, deposit, revocation, and fraud detection will follow the same procedures as in the home domain case, which greatly reduces the communication overhead in the system.

G. Inter-Domain Authentication from Mesh Router

Inter-domain authentication is more important for wireless peer-to-peer authentication networks. The mesh router generates and initialize the Defense ID for each client. The client first generates the Resistance ID and gives the resistance ID to mesh router. The mesh router receives that ID and registers the client resistance ID and send to home domain mesh routers. The mesh router sends the defense ID to client.

v.

IV. RESULTS AND DISCUSSION

CONCLUSION

In this system, we propose a hierarchical identity based cryptography architecture mainly consisting of the ticket based protocols, which resolves the conflicting sec- urity requirements of unconditional anonymity for honest users and traceability of misbehaving users. By utilizing the tickets, self-generated pseudonyms and the hierarchic-al identity based cryptography, the proposed architecture is demonstrated to achieve desired security objectives and efficiency.

H_0 : The data is normally distributed.
H_1 :The data is not normally distributed.
Table 4.1 shows that at 5 % level of confidence, the null hypothesis of normality cannot be rejected. KSE-100 index and macroeconomic variables inflation, exchange rate, oil prices and interest rate are normally distributed.
The descriptive statistics from Table 4.1 showed that the values were normally distributed about their mean and variance. This indicated that aggregate stock prices on the KSE and the macroeconomic factors, inflation rate, oil prices, exchange rate, and interest rate are all not too much sensitive to periodic changes and speculation. To interpret, this study found that an individual investor could not earn higher rate of profit from the KSE. Additionally, individual investors and corporations could not earn higher profits and interest rates from the economy and foreign companies could not earn considerably higher returns in terms of exchange rate. The investor could only earn a normal profit from KSE.

[1] I.F. Akyildiz, X. Wang, and W. Wang, "Wireless Mesh Networks: A Survey," Computer Networks, vol. 47, no. 4, pp. 445-487, Mar. 2005.

[2] Y. Zhang and Y. Fang, "ARSA: An Attack - Resilient Security Architecture for Multihop Wireless Mesh Networks," IEEE J. Selected Areas Comm., vol. 24, no. 10, pp. 1916-1928, Oct. 2006.

[3] M.G. Reed, P.F. Syverson, and D.M. Goldschlag, "Anonymous Connections and Onion Routing," IEEE J. Selected Areas Comm., vol. 16, no. 4, pp. 482-494, May 1998.

[4] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6, pp. 24-30, Dec. 1999.

[5] M. Raya and J-P. Hubaux, "Securing Vehicular Ad Hoc Networks," J. Computer Security, special issue on security of ad hoc and sensor networks, vol. 15, no. 1, pp. 39-68, 2007.

[6] Y. Zhang, W. Lou, W. Liu, and Y. Fang, "A Secure Incentive Protocol for Mobile Ad Hoc Networks," ACM Wireless Networks, vol. 13, no. 5, pp. 569-582, Oct. 2007.

[7] S.M.M. Rahman, A. Inomata, T. Okamoto, M. Mambo, and E. Okamoto, "Anonymous Secure Communication in Wireless Mobile Ad-Hoc Networks," Proc. First Int'l Conf. Ubiquitous Convergence Technology, pp. 131-140, Dec. 2006.

[8] A. Juels, M. Luby, and R. Ostrovsky, "Security of Blind Digital Signatures," Advances in Cryptology—Crypto '97, pp. 150-164, Springer-Verlag, 1997.

[9] 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.

.