Non-repudiation in pure mobile ad hoc network

Yi-Chi Lin

Jill Slay

lin, Y. C., & Slay, J. (2005). Non-repudiation in pure mobile ad hoc network. In *Proceedings of 3rd Australian Information Security Management Conference* (pp. 59-66). Edith Cowan University. Available here.
This Conference Proceeding is posted at Research Online.
https://ro.ecu.edu.au/ecuworks/7318

Non-Repudiation in Pure Mobile Ad Hoc Network

Yi-Chi Lin and Jill Slay
School of Computer and Information Science
University of South Australia
linyy021@students.unisa.edu.au

Abstract

Within the last decade, the use of wireless technologies has become more prevalent. Wireless networks have flexible architectures with data transferred via radio waves and can be divided into two categories; infrastructure-based wireless networks and mobile ad hoc network.

The mobile ad hoc network (MANET) is an autonomous system which can be dynamically built without pre-existing infrastructure or a trusted third party (TTP). Due to these infrastructure-less and self-organized characteristics, MANET encounters different problems from infrastructure-based wired network, such as key management, power shortage, and security issues. This paper will further divide MANETs into pure ad hoc networks which do not contain a TTP and organized ad hoc networks which contain an offline TTP, and then focus on the security issues especially the non-repudiation issue between two mobile nodes which communicate in pure ad hoc networks.

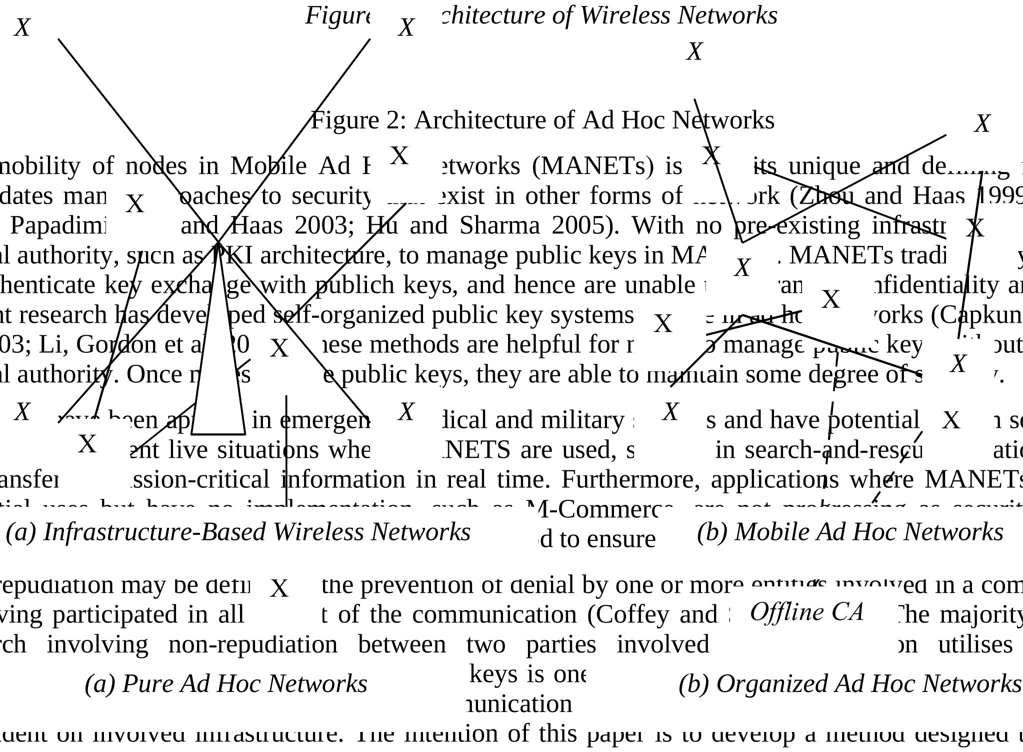
Keywords

Non-Repudiation, and Mobile Ad Hoc Networks

INTRODUCTION

In this paper, wireless networks can be divided into two categories; infrastructure-based wireless networks (see Figure 1.a) and mobile ad hoc network (see Figure 1.b). Furthermore, MANETs can be classified into pure ad hoc networks which do not contain a TTP (see Figure 2.a) and organized ad hoc networks which contain an offline TTP (see Figure 2.b).

Figur chitecture of Wireless Networks



(a) Infrastructure-Based Wireless Networks *(b) Mobile Ad Hoc Networks*

Figure 2: Architecture of Ad Hoc Networks

(a) Pure Ad Hoc Networks *(b) Organized Ad Hoc Networks*

The mobility of nodes in Mobile Ad H etworks (MANETs) is its unique and de feature, but invalidates man oaches to security exist in other forms of ork (Zhou and Haas 1999; Karpijoki 2001; Papadimi and Haas 2003; Hu and Sharma 2005). With no pre-existing infrastr there is no central authority, sucn as PKI architecture, to manage public keys in MA . MANETs tradi y are unable to authenticate key exchange with publich keys, and hence are unable an nfidentiality and security. Recent research has deve ped self-organized public key systems orks (Capkun, Buttyan et al. 2003; Li, Gordon et al 20 nese methods are helpful for r manage key out an existing central authority. Once n s e public keys, they are able to maintain some degree of s .

MA been ap in emergen lical and military s and have potential n several other field ent live situations whe NETS are used, s in search-and-rescu ations, require the transfer ssion-critical information in real time. Furthermore, applications where MANETs may have M-Commerce in online d to ensure

Non-repudiation may be defi the prevention of denial by one or more entities involved in a communication of having participated in all t of the communication (Coffey and he majority of current research involving non-repudiation between two parties involved on utilises public-key cryp keys is one f a node unication on-dependent on involved infrastructure. The intention of this paper is to develop a method designed to create an environment that enforces non-repudiation in pure ad hoc networks to ensure the fairness of online transactions and within the transfer of data between nodes. This protocol will be based on work by several other researchers, but will attempt to identify and incorporate the strengths of each, whilst identifying and mitigating any weaknesses that may be presented.

A non-repudiation protocol is comprised of two main components; non-repudiation of origin (NRO) evidence and non-repudiation of receipt (NRR) evidence (Zhou and Gollman 1996a; Zhou and Gollman 1996b; Zhou and Gollman 1997b). An NRO is signed by the originator with its secret key and can be viewed as evidence by the recipient, and a NRR is signed by the recipient with its secret key and can be viewed as evidence by the originator. Originators and recipients will be unable to take advantage of others when they obtain an NRR or NRO using a non-repudiation protocol which also can prevent malicious nodes from falsely denying previous actions.

To achieve non-repudiation between two nodes, a TTP is usually involved in situations when an injustice occurs. A TTP is a reasonable solution to solve disputes between two nodes in a wired network, but a TTP can not perfectly operate within a MANET environment, whose defining characteristic is no pre-existing infrastructure or trusted central authorities. Therefore, non-repudiation protocols which require the involvement of a TTP to solve the dispute are not suitable for use in MANET settings. Thus, a special non-repudiation protocol which can perfectly work without the involvement of a TTP (Markowitch and Roggeman 1999) must be adopted to achieve the fairness between two mobile nodes.

CURRENT RESEARCH

Published protocols from other researchers can be classified into two main categories: non-repudiation protocols which focus on specific areas, such as efficiency and the development of new protocols; ad hoc networks including areas such as security issues and routing subjects.

The research for these two aims is being developed independently, and there are few researchers that aim to merge these disparate requirements (Wang and Guo 2004).

Achieving fairness within wireless networks

The fair is defined as “at the end of the protocol, either an originator receives NRR evidence and a recipient receives the message and NRO evidence” (Kremer, Markowitch et al. 2002). Therefore, the fairness is an essential requirement of a transaction in any type of network. Keeping the fairness of the protocol is helpful for participants to complete procedures. No participant is willing to join in an unfair transaction neither in the real world nor in the electronic world.

A fair exchange protocol for use in a wireless network was developed by Wang and Guo (Wang and Guo 2004). This protocol establishes a pseudo-resilient channel which uses a cyclic resending method to ensure a message sent will arrive at the intended recipient or recipients. The protocol developed also uses a non-interactive verifying approach, an RSA-based convertible signature scheme, and a transparent TTP to reduce communication and computation consumptions. Although this protocol uses several computation saving policies, a transparent TTP is still required to solve any disagreement which may occur.

Four different sub-protocols discussed in this paper are:

Registration protocol: ensures Alice and Bob both have to register with the TTP to acquire certificates before performing this protocol.

Main protocol can guarantee that Alice and Bob will obtain non-repudiation evidence.

Recovery protocol is performed by Alice or Bob to obtain final non-repudiation evidence from the TTP when an error occurs.

Abort protocol can only be activated by Alice to abort the transaction.

On Demand Public Key Management for Wireless Ad Hoc Network

The private and public key pair is a prerequisite of any type of network including wireless ad hoc networks. Obtaining certificate public keys from other nodes in the same MANET is important for security issues, such as confidentiality issues, integrity issues and non-repudiation issues.

On demand public key management based on hop differences between nodes was proposed by Li, Gordon and Slay in (Li, Gordon et al. 2004). The protocol includes key generation, distribution, verification, and revocation within a pure ad hoc network. In this schema, the topology is defined by the proximity of nodes as:

1. **1-hop neighbors** are within each other’s transmission range

2-hop neighbors are beyond one hop distance but have at least one common 1-hop neighbour.

multi-hop nodes are more than two hops away from each other

Intermediate nodes are encouraged to participate in certificating procedures to update information about other nodes' public keys. The more procedures nodes are involved in, the more updated information they will obtain. The main contribution of this paper is that nodes will not only have the public keys of other nodes, but these will have been certified and recognized as genuine.

Probabilistic Non-Repudiation without Trust Third Party

Most of non-repudiation protocols are based on an adjudicator to estimate the validity of NRO and NRR evidence, and judge injustices between participants. The probabilistic non-repudiation protocol however does not need the involvement of a TTP to keep the fairness. This feature corresponds with the nature of pure ad hoc networks.

A novel fair protocol which can perform without a TTP was proposed by Markowitch and Roggeman (Markowitch and Roggeman 1999) to achieve non-repudiation between a client and a salesman in the electronic world.

The transaction processes are:

Client → Provider: Request for a service

Provider → Client: Service

Client → Provider: Payment (acknowledgement)

This is a great improvement for non-repudiation protocols which always rely on the involvement of a TTP (Coffey and Saidha 1996; Zhou and Gollman 1996a; Zhou and Gollman 1996b; Asokan, Schunter et al. 1997; Zhou and Gollmann 1997a; Zhou and Gollman 1997b). The fairness of this protocol is based on the random number n chosen by the originator of the transaction. Because the recipient of the transaction cannot obtain this number, this particular non-repudiation protocol is applicable for most situations.

The procedures are described in the following steps.

The recipient (Bob) determines the date D

Step 1. B → A sSK_B(request,B,A,D)

The originator (Alice): checks D

chooses n

computes the signed f1, : : :, fn

Step 2. A → B sSKA (fn(m),A,B,D)

Step 3. B → A sSKB(ack1)

Step 4. A → B sSKA (fn-1(m),A,B,D)

Step 5. B → A sSKB(ack2)

.

.

Step 2n -2. A → B sSKA (f2(m),A,B,D)

Step 2n-1. B → A sSKB(ackn-1)

Step 2n. A → B sSKA(f1(m),A,B,D)

Step 2n+1. B → A sSKB(ackn)

m= fn(m) fn-1(m) … f1(m).

NRO={NROi | i=1,…,n}, with NROi= sSKA (fi(m),A,B,D)

NRR=sSKB(ackn)

A Fair Non-Repudiation Protocol

NRO and NRR evidence are basic components for participants to verify the transaction. Furthermore, NRD and NRS evidence are proof of a transaction between nodes and a TTP. This evidence is essential components for non-repudiation protocols.

Zhou and Gollmann stated that “A fair non-repudiation protocol should not give the sender of a message an advantage over the receiver, or vice versa” (Zhou and Gollman 1996a). Researchers developed a non-repudiation protocol which needs the use of a TTP to judge a transaction and to keep the fairness between a sender and a receiver.

Four different types of evidence are proposed in this paper:

Non-repudiation of origin (NRO) is intended to protect against the originator’s false denial of having sent the message.

Non-repudiation of receipt (NRR) is intended to protect against a recipient’s false denial of having received the message.

Non-repudiation of delivery (NRD) is facilitated by evidence that the message was forwarded by the TTP.

Non-repudiation of submission (NRS) is intended to protect against the originator’s false denial of having submitted the message to the TTP.

At the end of the protocol, the sender obtains NRR evidence and the receiver obtains NRO evidence. NRD and NRS are the evidences which are created after the sender or receiver communicating with the TTP. These evidences are basic components for nodes to verify the transaction. NRO and NRR evidence is also used in the proposed method.

NON-REPUDIATION IN MOBILE PURE AD HOC NETWORKS

Notation

TTP: Trusted Third Party

SK$_P$: Secret Key of Principal P

PK$_P$: Public Key of Principal P

m: message

X → Y:m: Principal X sends message m to Principal Y

t: timestamp

ePK$_P$ (m): encrypt message m with Principal P’s public key

sSK$_P$ (m): message m is signed by Principal P’s secret key

Non-repudiation of Origin (NRO): NRO is a type of evidence for the recipient to protect against the originator’s false denial of having sent the message.

Non-repudiation of Receipt (NRR): NRR is a type of evidence for the originator to protect against the recipient’s false denial of having received the message.

Proposed Methodology

In the protocol discussed in (Li, Gordon et al. 2004), every node creates its own public key and secret key pair without any communication with a TTP. In this paper, the size of these keys is not restricted, and several key sizes may be used by different nodes concurrently. For example, Alice makes her own public and secret key pair in 512 bit and Bob makes his own public and secret key pair in 1024 bit. As long as they exchange their public keys with each other correctly, Alice can get Bob’s 1024 bit public key, and Bob will get Alice’s 512 bit public key. Alice then can sign the message by her 512 bit secret key, and Bob can use her 512 bit public key to verify the message. Alternatively, Bob can sign his message with his key, and this can be verified by Alice. The only disadvantage of using several key sizes is that all encryption is conducted at the lowest key size, negating the benefit of having a large key pair. However, the length of keys is not restricted for any reason. A node can decide the length of his or her own public and secret key pair in an ad hoc network.

After the procedures of the method proposed in (Li, Gordon et al. 2004), every node in the same ad hoc network will acquire the certificates of other nodes’ public key. Nodes are encouraged to become intermediaries in certificate procedures, because the more procedures they involved in, the more information (public key certificates) they can obtain. Alice is assumed to be the originator and Bob is assumed to be the recipient in this chapter.

Once a node obtains the public keys of other nodes, the probabilistic non-repudiation protocol (Markowitch and Roggeman 1999) is then appropriate for a pure ad hoc network to maintain fairness in transactions. An extra timestamp is applied to this protocol, and the usage of the timestamp is slightly modified to decrease the computational time. For example, Alice will only send timestamp t_1 during the transaction process instead of sending subsequent transactions (such as t_3 or t_5) as NRO evidence is combined with $sSK_A\,(f_1(m),A,B,D)\quad sSK_A\,(f_2(m),A,B,D)\quad \ldots\quad sSK_A\,(f_n(m),A,B,D,t_1)$. Therefore, Alice only needs one timestamp (t_1) in step 2 (as discussed below) to prove the time when the NRO evidence is created. On the other hand, Bob only sends timestamp t_2 with ack_1 to Alice in step 3 (as discussed below), rather than sending timestamps in all subsequent messages as NRR evidence is combined with $ack_1\quad ack_2\quad \ldots\quad ack_n$. Therefore, Bob only needs one timestamp (t_2) in step 3 (as discussed below) to prove the time when the NRO evidence is created. The timestamp refers to when the node signs the message. A timestamp can prevent not only replay attacks from other malicious nodes, but also NRO and NRR evidence from reuse.

The procedural details are as follows:

Step 1: B → A: $sSK_B(request,B,A,D)$

Bob uses his secret key SK_B to sign the requested data D. This creates $sSK_B(request,B,A,D)$ and is sent to Alice. When Alice receives $sSK_B(request,B,A,D)$, she will validate data D, chooses a random number n, and divides function *f* into n sub-functions, $f_1\;\; f_2\;\; \ldots\;\; f_{n-1}\;\; f_n$.

Step 2: A → B: $sSK_A(f_n(m),A,B,D,t_1)$

Alice first calculates message m by using sub-function fn() to obtain fn(m). Alice then uses her secret SKA to sign fn(m), data D and timestamp t1, giving $sSK_A(f_n(m),A,B,D,t_1)$, which is then sent to Bob.

Step 3: B → A: $sSK_B(ack_1,t_2)$

Bob receives $sSK_A(f_n(m),A,B,D,t_1)$ from Alice, and verifies it by Alice's public key. He then uses his secret key SK_B to sign ack_1 and timestamp t_2, giving $sSK_B(ack_1,t_2)$, which is then sent to Alice to be viewed as evidence for $sSK_A(f_n(m),A,B,D,t_1)$.

Step 4: A → B: $sSK_A(f_{n-1}(m),A,B,D)$

Alice first calculates message m by using sub-function $f_{n-1}()$ to obtain $f_{n-1}(m)$. Alice then uses her secret SK_A to sign $f_{n-1}(m)$, and data D, giving $sSK_A(f_{n-1}(m),A,B,D)$, which is then sent to Bob.

Step 5: B → A: $sSK_B(ack_2)$

Bob receives $sSK_A(f_{n-1}(m),A,B,D)$ from Alice, and verifies it by Alice's public key. He then uses his secret key SK_B to sign ack_2, giving $sSK_B(ack_2)$, which is then sent to Alice to be viewed as evidence for $sSK_A(f_{n-1}(m),A,B,D)$.

.

.

.

Step 2n-2: A → B: $sSK_A(f_2(m),A,B,D)$

Alice first calculates message m by using sub-function $f_2()$ to obtain $f_2(m)$. Alice then uses her secret SK_A to sign $f_2(m)$ and data D, giving $sSK_A(f_2(m),A,B,D)$, which is then sent to Bob.

Step 2n-1: B → A: $sSK_B(ack_{n-1})$

Bob receives $sSK_A(f_2(m),A,B,D)$ from Alice, and verifies it by Alice's public key. He then uses his secret key SK_B to sign ack_{n-1}, giving $sSK_B(ack_{n-1})$, which is then sent to Alice to be viewed as evidence for $sSK_A\,(f_2(m),A,B,D)$.

Step 2n: A → B: $sSK_A(f_1(m),A,B,D)$

Alice first calculates message m using sub-function $f_1()$ to get $f_1(m)$. Alice then uses her secret SK_A to sign $f_1(m)$, and data D, giving $sSK_A(f_1(m),A,B,D)$, which is then sent to Bob.

Step 2n+1: B → A: $sSK_B(ack_n)$

Bob receives $sSK_A(f_1(m),A,B,D)$ from Alice, and verifies it by Alice's public key. He then uses his secret key SK_B to sign ack_n, giving $sSK_B(ack_n)$, which is then sent to Alice to be viewed as evidence for $sSK_A(f_1(m),A,B,D)$.

Message $m= f_n(m) \quad f_{n-1}(m) \quad \ldots \quad f_1(m)$

$NRO=\{NRO_i+NRO_n \mid i=1,\ldots,n-1\}$, with $NRO_i= sSK_A(f_i(m),A,B,D)$, and $NRO_n=sSK_A(f_n(m),A,B,D,t_1)$

$NRR=\{NRR_1+NRR_i \mid i=2,\ldots,n\}$, with $NRR_i = sSK_B(ack_i)$ and $ack_i=(i,B,A,D)$; $NRR_1=sSK_B(ack_1,t_2)$ and $ack_1=(1,B,A,D)$

At the end of this protocol, Bob (recipient) will obtain message m and NRO evidence, and Alice (originator) will obtain NRR evidence.

DISSCUSSION

The protocol proposed is similar to that discussed by Wang and Guo (Wang and Guo 2004), but offers distinct advantages within a MANET environment. Unlike Wang and Guo's implementation, this protocol does not rely upon use of a TTP to ensure fairness within a transaction between two nodes. This makes the proposed protocol applicable for use in pure ad hoc networking environments.

The protocol proposed in this paper places emphasis on what nodes can do after receiving the certificated public and secret key pair, and is inspired by traditional non-repudiation protocols (Coffey and Saidha 1996; Zhou and Gollman 1996a; Meng, Wang et al. 2002; Ray and Ray 2002)to consider the issues associated with non-repudiation within pure ad hoc networks. Although a TTP is a practical solution to solve a dispute between two nodes, fixed infrastructure is not applicable in a pure ad hoc network topology. Some existing non-repudiation protocols (Zhou and Gollman 1996b; Zhou and Gollman 1997b) also require Non-Repudiation of Delivery (NRD) evidence and Non-Repudiation of Submission (NRS) evidence to prove the communication actually occurred between nodes and a TTP, in addition to the NRR and NRO evidence required by other non-repudiation protocols (Zhou and Gollman 1996a; Zhou and Gollmann 1997a). The major difference between the proposed non-repudiation method and the method developed by Li, Gordon and Slay in (Li, Gordon et al. 2004) is the proposed solution focuses on the non-repudiation of the communication rather than the issues associated with key management. This protocol assumes that key management has occurred, and hence may rely upon systems discussed by other authors.

The proposed method does not encounter the same issues as traditional non-repudiation protocols (Coffey and Saidha 1996; Zhou and Gollman 1996a; Zhou and Gollman 1996b; Asokan, Schunter et al. 1997; Zhou and Gollmann 1997a; Zhou and Gollman 1997b) including area such as computational complexity with a TTP, as it is particularly designed for use within pure ad hoc networks, unlike other methodologies, which are adapted to pure ad hoc use after being primarily designed for infrastructure-based networks.

The use of NRD and NRS evidence is avoided in the design of the proposed solution, as the use of these in addition to NRR and NRO evidence increases the computational complexity of the protocol, and the use of lightweight protocols is favored in MANET development. In this situation, nodes will have non-repudiation insurance whilst retaining the benefits of a pure ad hoc network.

The key of the proposed method is that the originator secretly chooses a random number n before sending data, and the recipient does not know this random number. The originator and the recipient are unable to take any advantage of each other given this assumption. The originator hopes the data will be sent completely, and that the transaction is not interrupted. Similarly, the recipient wishes the protocol finished without interruption as the transaction must complete for the information to be deciphered. Therefore, neither the originator nor the recipient will terminate the transaction arbitrarily. The only way for the recipient to obtain data without sending an NRR is to guess the random number n. If the recipient is able to determine the random number n, he or she can terminate the procedure at step 2n (as the recipient can decipher message m by combining the received data f_1, f_2,… , f_{n-1}, f_n), without activating step 2n+1 (therefore originator will not get ack_n, he can not get NRR by combining ack_1, ack_2,…, ack_{n-2}, ack_{n-1}). The final result in this situation is that the recipient receives the message m, but the originator does not receive the NRR evidence. This breaches the fairness between the originator and the recipient. However, this protocol relies on the fact that the recipient does not know when the last step (random number n) occurs.

Due to this reliance on keeping the random number unknown to the recipient, this protocol still has a chance of failure, and hence is more suited to low value transactions than high value ones. Despite this reliance, this method represents a reasonable solution to solve the dispute in a pure ad hoc network with particular characteristics.

CONCLUSION

The intention of this paper is to focus on the non-repudiation between originators and recipients within pure MANETs. Communications and transactions in MANETs are not completely reliable for nodes due to the nature of the networks. The application of the probabilistic non-repudiation protocol, adapted to perform without a TTP, allows nodes not only to communicate safely with each other in MANETs, but also for non-repudiation evidence after data exchange.

REFERENCES

COPYRIGHT