ISSN (Online) 2278-1021
ISSN (Print) 2319-5940

IJARCCE

International Journal of Advanced Research in Computer and Communication Engineering

nCORETech

LBS College of Engineering, Kasaragod

Vol. 5, Special Issue 1, Feburary 2016

Cost-effective and Secure Data Sharing in MANET

Lincy M[1], Anju J[2]

PG Scholar, Department of Computer Science, LBS College, Kasaragod, India[1]

Assistant professor, Department of Computer Science, LBS College, Kasaragod, India[2]

Abstract: Wireless mobile Ad Hoc Networks (MANETs) are gaining popularity in the area of mobile computing. MANETs face security problems because of their unique characteristics like mobility, dynamic topology and lack of central authority and infrastructure support. In traditional networks, deploying a powerful and reliable security scheme such as Public Key Infrastructure (PKI) needs a central authority or trusted third party to ensure fundamental security services including digital certificates, authentication and encryption methods. In the proposed scheme, a secure identity-based anonymous and authentication scheme is proposed for networks without any PKI and a cost-effective light weight encryption scheme for ensuring confidentiality is also proposed.

Keywords: Authentication, Encryption, MANET, P-coding, Forward security.

I. INTRODUCTION

Mobile adhoc networks are self-configuring networks of mobile nodes without any support of a central authority, e.g., a central server. Without a central administration, packets are forwarded from one device to another by the mobile nodes within the network. This means that each node acts as both a host and a router. Since nodes have to depend on each other to forward the packets to destinations, several issues need to be considered such as routing, battery life, data confidentiality. Authenticity e.t.c.

A crucial issue in MANETs is how to limit the energy usage in order to preserve a longer life span for mobile nodes. Several energy-efficient schemes are proposed to solve these issue [2], [3], and [4]. The energy saving comes from fact that less transmissions are required when in-network nodes are enabled to encode packets. Other than transmission cost, there are other sources of energy consumption, e.g., data encryption/decryption. Here we propose P-Coding, a lightweight encryption scheme to provide confidentiality for network-coded MANETs in an energy-efficient way. The concept of P-Coding is to let the source randomly permute the symbols of each packet (which is attached with its coding vector), before performing network coding. Without knowing the permutation, intruder cannot locate coding vectors for correct decoding. Authentication is simply a process carried out by two entities in order to identify one another. Without authentication, an unauthorized mobile node could easily access and use the available resources within the network. Therefore, it is essential to have a mechanism for preventing an “outsider” from accessing the network Widely used authentication mechanisms in conventional wired networks is the public key management system using certificates. the main issues to consider in a certificate-based scheme is the secure distribution of the public keys to all the nodes in the network. The Public Key Infrastructure (PKI) [1] defines methods to handle public key management using X.509 certificates. In a wired network, there exists a centralized certificate server which handles the creation, renewal and revocation of certificates. This is not feasible in ad hoc networks, due to the absence of a fixed infrastructure and centralized management. Besides, due to the dynamic topology of the network, frequent link failures may occur, resulting in issues such as re-authentication and timely communication with the certificate server.

Ring signature is a promising method to construct an anonymous and authentic data sharing system. It permits a data owner to anonymously authenticate his data. Still the costly certificate verification in the traditional public key infrastructure (PKI) setting becomes a hindrance for this solution to be scalable. Identity-based (ID based) ring signature, which eliminates the process of certificate verification, can be used instead.

Then enhance the security of ID-based ring signature by providing forward security: If a secret key of any user has been compromised, all previous generated signatures that include this user still remain valid.

Our contribution is two-fold: 1) we propose a new encryption scheme which is lightweight in computation 2) we present a mechanism for ensuring authenticity and anonymity with forward security and the mathematical assumption. In the rest of the paper, we first briefly review existing encryption and authentication mechanisms and their problems. Then, in Section 3, we describe our proposed system. Mathematical assumptions are presented in Section 4. Section 5 discusses the protocol, followed by the conclusion.

DOI 10.17148/IJARCCE

II. RELATED WORK

A number of related works can be seen in both encryption schemes and anonymous authentication schemes. Most influenced works are discussed here. One scheme in light weight encryption is SPOC [2], proposed by Vilela et al., in which the source encrypts/locks the GEV (Global Encoding Vector) of each message after random linear coding, and attach another set of GEVs. Receivers can recover the source messages by following a decode-decrypt-decode procedure. This scheme is essentially an end-to-end cryptographic approach, and is lightweight in computation. Another scheme proposed by Fan et al. [3] is based on Homomorphism Encryption Function (HEF) [4]. This scheme has the coding coefficients encrypted using HEF. Due to the homomorphism property of HEF, linearly combination operations can be directly performed on the encrypted coding coefficients. As a result, no extra coding coefficients are needed as by SPOC. As another difference from SPOC, Fan’s HEF-based scheme can achieve both content secrecy (i.e., confidentiality), and contextual secrecy (i.e., privacy) at the same time.

Rivest, Shamir and Tauman [7] first introduced the notation of ring signature, where a signer, ad hoc determining a group of users including himself, signs a signature on behalf of the group such that a verifier will be convinced that the message was really signed by one of the members of the group, but he cannot identify the actual signer.

There exist several ID-based ring signature schemes from pairings like [8, 9], where the computation of pairing is the most time-consuming. However, the number of pairing computations of most [10, 11] of the existing ID-based ring signatures grows linearly with the size of the group.

The first ID-based ring signature scheme claimed to be secure in the standard model is due to Han et al. [12] under the trusted setup assumption.

However, their proof is wrong and is pointed out by [13].

III. PROPOSED WORK

Light-weight encryption scheme in network coded MANET

Network coding is a particular in-network data processing technique that exploits the characteristics of the wireless medium(in particular, the broadcast communication channel)in order to increase the capacity or the throughput of the network.

Suppose a source s need to transmit a message to destinations T. Assuming nodes in the network can only perform routing, i.e., replicate and forward, received messages, the multicasting will take place in a sequence of steps. In each step, a node, having received the packet so far, forwards the packet to some neighbors at a certain power level. Due to the broadcast nature of radio transmissions, a single transmission by a certain transmission may successfully reach multiple nodes. The problem is to find a group of relaying nodes and their respective power levels such that all nodes in T receive the message, whereby the total energy expenditure for the task is reduced. By this formulation, it can be easily concluded that the optimal forwarding scheme should be based on a tree structure. Still we need to improve the conventional formulation to achieve a potentially lower energy per bit.

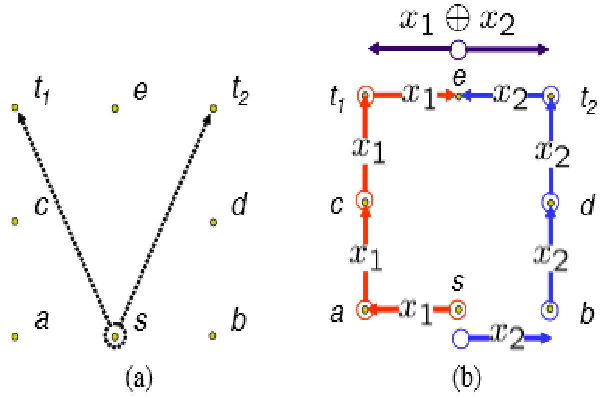

Fig .1 Example illustrating how network coding reduces transmission times in MANETs.(a)without network coding,(b)with network coding. Adapted from ‘‘Minimum-Energy Multicast in Mobile Ad Hoc Networks using Network Coding”, by Y. Wu, P. Chou, and S. Kung, IEEE Trans.Commun., vol. 53, no. 11, pp. 1906-1918, Nov. 2005.

DOI 10.17148/IJARCCE

In Fig.1, the minimum amount of energy required to deliver 1 message from s to {t1, t2} is 5 (transmissions) using the conventional routing approach, whereas 2 messages can be delivered with 9 transmissions using network coding.
Fig.1 (a): An example wireless adhoc network. The locations of the nodes have been marked with dots. Assume each node is equipped with a transmitter operating at a fixed transmission range, which is just sufficient to reach its lateral neighbors, but not the diagonal ones. Under this setting, each physical layer transmission consumes a unit amount of energy It is easy to see that the minimum amount of energy required to deliver 1 message From s to {t1,t2} is 5 (transmissions) using the conventional routing approach. One such solution is as follows: first s broadcasts the message to {a,b} using on transmission; next a forwards it to c, c forwards to t1,b forwards to d ,and d forwards to t2.(b):Minimum energy multicast with network coding on this example network. Suppose s has two messages,x1 and x2. First x1 is delivered to t1 with 3 transmissions and x2 is delivered to t2 with 3 transmissions. Next t1 transmits x1to e and t2 transmits x2 to e. The critical step occurs at e, which broadcasts the XOR-ed result of two messages, x1x2, to t1 and t2, consuming only one transmission. Each of the two destinations can recover both x1 and x2 by solving a simple linear system of equations.

1. System Model

We consider a typical MANET consisting of N nodes, each of which can be a source. The MANET can be modeled as an acyclic directed graph G = (V,E). For each node v ϵ V, there is a link from v to u if u is within v’s transmission range. Let Γ^- (v) be the set of links terminating at v, and Γ^+(v) be the set of links originating from v. We assume that each link e ϵ E has the capacity of one packet per unit time, and y(e) is the packet carried on it. Here a packet is defined as a row vector of l elements from finite field Fq. We also assume that linear network coding is enabled in this network. To illustrate how network coding works, let us consider the case that one node s needs to deliver a series of packets $x_i, \dots, x_h$ to a set of sinks T C V . Define the matrix of source packets as X =$[x_i^T, \dots\dots, x_h^T]^T$, i.e., X consists of all source packets as its rows. For simplicity, let Γ^-(s) consists of h imaginary links, $\breve{e}^1, \dots, \breve{e}^h$, with $y(\breve{e}^i)$= xi. Then for any e $\epsilon\Gamma^+$ (v), v ∉T, y(e) is calculated by linearly combining the incoming packets of v as

$$y(e) = \sum_{e' \epsilon \Gamma^-(v)} \beta_{e'}(e) y(e') = \beta(e)[y^T(e')]^T_{e' \Gamma^-(v)} \quad (1)$$

where the coefficients $\beta_{e'}$ are chosen over Fq, and the row vector $\beta(e) = [\beta_{e'}]_{e' \epsilon \Gamma^-(v)}$ is termed as the Local Encoding Vector (LEV) of link e. By induction, y(e) can be represented as the linear combination of source packets

$$y(e) = \sum_{i=1}^{h} g_i(e) x_i = g(e)X \qquad (2)$$

where g(e) = $[g_1(e), \dots, g_h(e)]$ can be calculated recursively using Eq. (1), and is termed as the Global Encoding Vector (GEV) of link e. Assume that h packets received by a sink node v from links $e_1, \dots, e_h$. Then, by applying Eq. (2), we have,

$$Y = \begin{pmatrix} y(e_1) \\ \cdot \\ \cdot \\ y(e_h) \end{pmatrix} = \begin{pmatrix} g(e_1) \\ \cdot \\ \cdot \\ g(e_h) \end{pmatrix} X = GX \qquad (3)$$

where G is termed as the Global Encoding Matrix (GEM) of node v. Since G is invertible with high probability when q is sufficiently large [13], v can reconstruct source messages X by calculating $X = G^{-1}Y$.
In practice, the source prefixes each packet xi with the
i^{th} unit vector ui,

$$[u_i, x_i] = \left(\underbrace{0,\dots,0}_{i-1},1,\underbrace{0,\dots\dots,0}_{h-I},x_{i,1},\dots,x_{i,l} \right) \qquad (4)$$

where each ui is termed as a tag. With the same coding operations performed on these tags, each packet will automatically contain its GEV.

2. P-coding: the proposed scheme

This section defines permutation encryption, based on which we introduce P-Coding, a lightweight encryption scheme. We formalize the concept of permutation encryption as a special case of the classic transposition cipher [15]. We term a sequence Лcontaining each element of set 1, . . . , n. once and only once as a permutation with length n. Let Л(i) be the ith element of Л, then the product of two permutations Л$_1$ and Л$_2$, defined by Л$_1$oЛ$_2$,is calculated using Л$_1$Л$_2$(i) =Л$_1$(Л$_2$(i)) Let Л$^{-1}$ be the inverse of Лwith respect to product operation

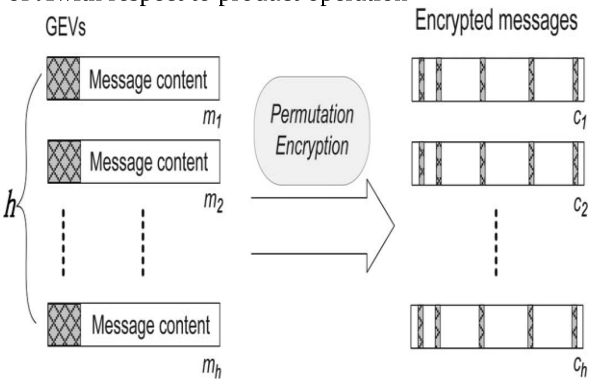

Fig.2 Permutation encryption on coded messages.

Adapted from “A Lightweight Encryption Scheme for Network-Coded Mobile Ad Hoc Networks” by Peng Zhang, Chuang Lin, Senior Member, IEEE, Yixin Jiang, Yanfei Fan, and Xuemin (Sherman) Shen, Fellow, IEEE, IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 9, SEPTEMBER 2014

The basic idea of P-Coding is to perform permutation encryptions on coded messages, as shown in Fig. 2. After PEF operations, symbols of the messages and corresponding GEVs can be mixed and reordered together. The P-Coding scheme primarily consists of three stages: source encoding, intermediate recoding, and sink decoding. Without loss of generality, we assume that there is a Key Distribution Center (KDC) responsible for symmetric key establishment, so that the source and sinks can share a PEF key k at the bootstrap stage of P-Coding.

2.1 Source Encoding Consider the situation that a source s has h messages, denoted by column vectors x1, . . . , xh, to be sent out. It first prefixes these h messages with their corresponding unit vectors, according to Eq. (4). Then the source performs linear combinations on these messages with randomly chosen LEVs. For instance, with LEV β(e$_i$) of output link ei, we can get the coded message y(ei) = [β (ei), B(ei)X], where X =[x_i^T,……...,x_h^T]^T. Finally, the source performs permutation encryption on each message y(ei) to get its ciphertext c[y(ei)] = Ek[y(ei)].

2.2 Intermediate Recoding Since the symbols of messages and corresponding GEVs are rearranged via PEF, and the intermediate nodes have no knowledge of the key being used, it is rather difficult for them to reconstruct source messages. On the other hand, as permutation encryptions are exchangeable with linear combinations, intermediate recoding can be transparently performed on the encrypted messages.

$$C\,[\,y(ei)\,] = c\left(\sum\nolimits_{e'\epsilon\Gamma^-(v)} \beta_{e'}(e)y(e')\right) = \sum\nolimits_{e'\epsilon\Gamma^-(v)} \beta_{e'}(e)c[y(e')]$$

This transparency property makes P-Coding rather efficient, since no extra effort is needed at any intermediate node.

2.3 Sink Decoding

For each sink node, on receiving a message c[y(e$_i$)]from its incoming link ei $\epsilon\Gamma^{-(}$v), it decrypts the message by performing permutation decryption on it Dk{ c[y(ei)] } = Ek^{-1} { Ek [y(ei)] } = y(ei) Once h linearly independent messages y(e1), . . . , y(eh) are collected, the sink derives the following matrix representation similar to 3:

$$Y = \begin{pmatrix} y(e_1) \\ . \\ . \\ y(e_h) \end{pmatrix} = \begin{pmatrix} g(e_1),\ g(e_1)X \\ . \\ . \\ g(e_h),\ g(e_h)X \end{pmatrix} = [G,\ GX]$$

Finally, the source messages can be recovered by applying Gaussian eliminations on Y

$$Y = [\ G,GX\ ] \xrightarrow[\text{elimination}]{\text{guassian}} [\ I\ ,X\ ]\ .$$

B . Anonymity and Authentication scheme

Group signatures, introduced by Chaum and van Heyst [14], provide anonymity for signers. Any member of the group can sign messages, but the resulting signature keeps the identity of the signer secret.

i. ID-Based Signature

Identity-based (ID-based) cryptosystem, introduced by Shamir [14], eliminated the need for verifying the validity of public key certificates, the management of which is both time and cost consuming. In an ID-based cryptosystem, the public key of each user is easily computable from a string corresponding to this user's publicly known identity (e.g., an email address, a residential address, etc.). A private key generator (PKG) then computes private keys from its master secret for users. This property avoids the need of certificates which are necessary in traditional public-key infrastructure) and associates an implicit public key (user identity) to each user within the system. In order to verify an ID-based signature, different from the traditional public key based signature, one does not need to verify the certificate first. The elimination of the certificate validation makes the whole verification process more efficient, which will lead to a significant save in communication and computation when a large number of users are involved.

ii. Forward Security

In practice the greatest threat against the security of a digital signature scheme is exposure of the secret (signing) key, due to compromise of the security of the underlying system or machine storing the key. The danger of successful cryptanalysis of the signature scheme itself is hardly as great as the danger of key exposure, as long as we stick to well-known schemes and use large security parameters. The most widely considered solution to the problem of key exposure is distribution of the key across multiple servers via secret sharing [18,5]. There are numerous instantiations of this idea including threshold signatures [7] and proactive signatures [14]. Distribution however is quite costly. While a large corporation or a certification authority might be able to distribute their keys, the average user, with just one machine, does not have this option. Thus while we expect digital signatures to be very widely used, we do not expect most people to have the luxury of splitting their keys across several machines. Furthermore even when possible, distribution may not provide as much security as one might imagine. For example, distribution is susceptible to common-mode failures: The goal of forward security is to protect some aspects of signature security against the risk of exposure of the secret signing key, but in a simple way, in particular without requiring distribution or protected storage devices, and without increasing key management costs.The concept was first suggested by Anderson [2], and the solutions were designed by Bellare and Miner [7].

The idea is dividing the total time of the validity of a public key into T time periods, and a key compromise of the current time slot does not enable an adversary to produce valid signatures pertaining to past time slots.

IV. SYSTEM SETUP

A. Signature scheme

- Setup: On input an unary string 1^ɤ where ɤ is a security parameter, the algorithm outputs a master secret key msk for the third party private key generator and a list of system parameters param that includes ɤ and the descriptions of a user secret key space Ƿ, a message space M as well as a signature space Ψ.
- Extract:On input a list param of system parameters,an identity IDi ϵ {0,1}* for a user and the master secret key msk, the algorithm outputs the user's secret key ski;0 ϵD such that the secret key is valid for time t = 0. In this paper, we denote time as nonnegative integers. When we say identity IDi corresponds to user secret key ski;0 or vice versa, we mean the pair (IDi; ski;0) is an input-output pair of Extract with respect to param and msk.
- Update: On input a user secret key ski;t for a time period t, the algorithm outputs a new user secret key ski;t+1 for the time period t+1.
- Sign : On input a list param of system parameters, a time period t, a group size n of length polynomial in ɤ, a set L = (IDi ϵ{0; 1}*|iϵ[1,n]} of n user identities, a message m ϵ M, and a secret key skЛ;tϵƷ; Лϵ[1,n] for time period t, the algorithm outputs a signature σϵ Ψ
- Verify: On input a list param of system parameters, a time period t, a group size n of length polynomial in ɤ, a set L={IDi ϵ{0,1}*|iϵ[1,n]} of n user identities, a message m2M, a signature σϵΨ, it output either valid or invalid.

V. DISCUSSION

This project ensures a cost-effective data sharing through a cost-effective encryption scheme and a cost-effective anonymity and authentication scheme. Here we are using a simple and effective columnar transposition cipher with permutation encryption. It is less in computation cost than other encryption schemes.

We compare our scheme with related work in terms of features, computation, and space requirement, the verification for non ID-based 1-out-of n ring signature schemes require additional certificate verification for n users. We exclude the cost and space for those n certificates verification in this comparison, as it may vary in different scenarios.

VI. CONCLUSION

We proposed P-Coding, a lightweight encryption Scheme. P-Coding is efficient in computation, and incurs less energy consumption for encryptions/decryptions. Also we have proposed an efficient ID-based ring signature scheme with a notion called forward secure ID-based signature. It allows an ID-based ring signature scheme to have forward security. Our scheme provides unconditional anonymity and can be proven forward- secure unforgeable in the random oracle model.

REFERENCES

[1]. Peng Zhang, Chuang.Lin,Senior Member,IEEE,Yixin jiang,Yanfei Fan, and Shen, "Cost-effective Anonymous and Authentic Data Sharing with FForward Security" IEE Transaction on Parallel and Distributed computing, vol. 25,NO.9 Sept 2014.
[2]. J.P Vilea,LL.Lima,and J.Barros,"Light weight security for network Coding,"in Proc.IEEEIC,May2008,pp.2213-2221.
[3]. Y.Fan,Y.jiang,H.zhu,and X.shen,"An Efficient Privacy Presrving scheme Against traffic analysis in Network Coding,"in Proc.IEEEINFOCOM,Apr.2009,pp.2213-2221.
[4]. J.Benaloh,"Dense Probabilistic Encryption," in Proc.Workshop Sel.Areas Cryptogr.,Aug.1996,pp,120-128
[5]. K.Yang and X.Jia"An Efficient and Secure Dynamic Auditing Protocolbfor Data Storage in Cloud Computing",IEEE Trans.Parallel and Distributtive Systems,vol.24.no.9.pp.1717-1726 2013
[6]. Xinyil huang,Joseph "EEfficient and secure Dynamic Auditing protocol.2013.
[7]. D.Boneh,X.Boyen,and H.Shacham,"Short group signatures:,in PProc.Annu.Int.Cryptol.conf.adv.Cryptol.2004,vol.3152
[8]. S.S M.Chow,S.M YIU,and L.C.K.Hui"Effficien iidentiy based ring signature"2005,vol.3631,pp.499-512.
[9]. J.Han,Q,Xu and g,cham,"Efficient id-based threashold ring signature scheme"in 2008,pp437-442
[10]. J.hermax and G.sian "Forking Lemma as for ring signature scheme in 4th Int.conf.India,2003,vol.2904
[11]. H.XionZ.Qin,and.Li"An anonymous sealed-bid electronics auction based on ring signature vol.8,no.3.pp.235-242
[12]. J.zan"An efficient identity based ring signature scheme and extension in proc.In.conf.comput.Sci.Appril 2007.vol-4706
[13]. J.Yu.R.Hao,F.Kong"Forward secure Identity based signature"IEEE Trans.vol.181./no.3
[14]. G.Yan,D.Wen,S.Olariu and M.Wegle,"Seecurity challenges in vehicular,cloud,computing",IEEE Trans.Vol.14.pp.284.Mar2013

DOI 10.17148/IJARCCE