iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 5 **Issue:** X **Month of publication:** October 2017

DOI: http://doi.org/10.22214/ijraset.2017.10226

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor:6.887
Volume 5 Issue X, October 2017- Available at www.ijraset.com

Sub-Group Operations in Manet Using Bivariate Polynomial

Manohar Sai[1], N Chaitanya Kumar[2]
[1, 2] M.Tech, JNTU Hyderabad

***Abstract**: Mobile ad-hoc networks are dynamic in nature, resource constraint and vulnerable to security threats due to the absence of centralized infrastructure. It is always a challenging task to secure communication between nodes of the MANET and in sub-groups of the MANET. MANET adopts two kinds of approaches Public key cryptography and Identity based cryptography. In this paper, we propose a novel method that employs public key cryptography techniques to perform sub-group operations efficiently in MANET. In Public Key Infrastructure(PKI), the Central/Certificate Authority(CA) manages the keys, but in MANET there is no CA, we need to distribute the role of CA to the nodes itself. We adopt distributed Public Key Infrastructure (PKI) in setting up of the MANET. For this purpose, we employ symmetric bivariate polynomial along with secret sharing technique.*

***Keywords**: MANET, bivariate polynomial, subgroups, secret sharing technique, threshold cryptography, public key infrastructure*

I. INTRODUCTION

Mobile ad-hoc network is a infrastructure-less, self-organized, dynamic and resource constraint network [1]. The participating entities are known as mobile nodes. These nodes roam freely and every node has its own communication range [2]. If two or more node's communication range overlap, then nodes can communicate with each other. Due to the dynamic nature of the network, new nodes join, some nodes may leave the network and few may fail to function. The nodes are energy limited as they are battery powered devices. Many security threats exist to MANETS such as eaves-dropping, interception, denial of service and routing attacks [3][4]. Public Key Infrastructure (PKI) [5] uses encryption and authentication by digital certificates for a secure communication. The distributed Public Key Infrastructure is adopted in this paper, to make the MANET completely de-centralized. A (t, n) threshold scheme[6][7][8] is applied in distributing CA power to the nodes of the MANET [9]. In our proposal, we discuss a technique to perform sub-group operations efficiently and suggest a certification scheme for sub-groups derived from BLS signature scheme[10].

A. Attacks on MANET [11]

In MANETS, there are two types of attacks namely Active and Passive. Passive attacks capture information in transmission and active attacks cause damage to the network by interrupting the normal flow of operations. Harmful/Malicious nodes cause both active and passive attacks. A malicious node does not authenticate itself to other nodes. Since the mobile nodes share a wireless medium, the messages transmitted can be eavesdropped or fake messages may be injected. As one-hop connectivity is maintained among neighbouring nodes, the attacker can perform traffic analysis and traffic monitoring attacks. Other attacks such as denial of service and SYN flooding can also take place.

B. Distributed PKI

Public key cryptography(PKC)[12] provides security services such as confidentiality, integrity, authentication, non-repudiation, encryption and digital signatures. Public key infrastructure(PKI)[5] manages digital certificates that are important in establishing public key cryptography. In Public Key Infrastructure(PKI), a central/certificate authority(CA) has the sole power to issue certificates and maintain keys. The CA has a secret key '*s*', which it uses to sign the certificates. In MANET, the role of the CA cannot be assigned to a single node, as it may leave the network or fail to function. So the role of the CA has to distributed to the nodes of the MANET [9], this is achieved using a (t,n) threshold secret sharing scheme, where the MANET secret '*s*' is distributed as shares to the nodes.

C. Threshold Cryptography

As MANET is a decentralized network, the master secret key '*s*' of the PKI is distributed among the nodes of the MANET using secret sharing scheme. One such secret sharing technique is the Shamir's secret sharing scheme[8]. In this scheme, a dealer

©IJRASET (UGC Approved Journal): All Rights are Reserved

distributes a secret '*s*' among n entities. Each entity receives a share privately from the dealer. To reconstruct the secret 's', it uses a (t, n) threshold access structure, where t out of n shares are required. Shamir's secret sharing scheme can be adopted to MANETS. The role of the dealer is distributed to the nodes of MANET itself. This is achieved by using a symmetric bivariate polynomial.

D. Related Work

One common issue faced by MANET when applying cryptography is, how to distribute the role of CA or trusted authority, many proposals use secret sharing technique to distribute secret key '*s*' of CA or trusted authority to secure MANET. Zhou and Haas[6] were the first to propose distributed CA for MANETS. Kong et al.[13] also worked on a similar technique to distribute trust among the nodes. However, their particular RSA threshold scheme was proved insecure[14][15]. In previous works, bi-variate polynomials have already been used to dynamically to allow new nodes joining the network without the need of any external trusted entity[16]. Anzai et al.[17] and Herranz et al.[18] constructed decentralized, flexible, dynamic group key distribution schemes by using polynomials in two variables. Saxena et al.[19] used similar procedure to set up pairwise keys in a non-interactive approach for a mobile ad-hoc setting.

Aggregate signature algorithm for MANET was proposed by Daxing et al. [20] using bilinear pairing and Multi user setting signature with tight security was proposed by Hanaoka et al. [21] based on BLS signature [10].

Our work is extension to node authentication using BLS signature by nc kumar et al.[22] and related to the cryptographic techniques proposed for MANETs by Herranz et al. [18]. Our paper proposes the use of bivariate polynomial over a trivariate polynomial to perform subgroup operations. The authors in [18] have used trivariate polynomial to perform subgroup operations. In our proposal, we run the same protocol as in setup phase to perform subgroup operations. This reduces the computational overhead and also the signature algorithm used is from nc kumar et al.[22] which is lightweight.

II. SELF-ORGANIZED PKI AND SECRET SHARING TECHNIQUE

In self-organized PKI for MANETS, the role of Public Key Infrastructure is completely distributed among the nodes of the MANET using shamir secret sharing scheme [8]. Blakley [7] and Shamir [8] were the first to introduce secret sharing techniques. A secret sharing scheme contains a dealer and a set $P = \{p_1, p_2,..., p_n\}$ of n participants. The dealer has a secret 's' and wants to distribute the share of the secret corresponding to the participant pi privately. A valid subset p (for : $p \subset P$) of atleast t number of participants holding valid partial shares can reconstruct the original secret 's'. The t is called threshold number and (t, n) is called as the threshold access structure[8]. In our paper, we use Shamir's secret sharing technique that uses a (t, n) threshold access structure[8]. Shamir's secret sharing scheme uses (t, n) threshold access structure by polynomial interpolation. Let Z_q be a finite field with $q > n$ and let 's' $\in Z_q$ be the secret. The dealer picks a polynomial P(x) of degree at most t−1, where the constant term of P(x) is 's' and alother coefficients of P(x) are selected uniformly and independently at random from Z_q. i.e.,

$$P(x) = s + \sum_{i=1}^{t-1} a_i x^i .$$

Every participant p_i is publicly associated to a field element a_i. Distinct participants are mapped to distinct field elements. The dealer privately sends to participant u_i the value $s_i = P(a_i)$, for i = 1, 2,…., n. Without loss of generality, we can assume that the set of participants willing to recover the secret 's' is $p_1, p_2,..., p_n$. The secret 's' can be obtained as

$$\sum_{i=1}^{t} \lambda_i s_i \quad \text{for} \quad \lambda = \prod_{j \neq i} \frac{a_j}{a_j - a_i}$$

are the Lagrange coefficients. It is proven that any combination of less than t participants obtain no information about 's'.

III. OUR PROPOSAL

This section is divided into three major phases namely Setup, Key Generation, Subgroup operations.

A. Setup

In this phase every node n_i receives partial share s_i of the MANET secret 's'. There are some parameters that are public: an additive group G of prime order q, generated by some element P and a collision-resistant hash functions h:(0,1)*→Z_q, where we assume that the discrete logarithm problem (i.e., computing the integer 's' from the value sP) is hard [21]. The following protocol is run by the nodes.

©IJRASET (UGC Approved Journal): All Rights are Reserved

1) Let n be the number of nodes in the MANET, t be the threshold and k be the founding number of nodes for $t \leq k \leq n$.
2) Every founding node chooses a bivariate polynomial $f_i(x, z)$, symmetric in x, z and the max degree of polynomial is t-1.
3) Every node n_i computes $f_{ij}(h(n_j), z)$ for all other founding nodes and itself, $1 \leq i,j \leq k$.
4) Now every node secretly sends computed $f_{ij}(h(n_j), z)$ to corresponding node n_j . Furthermore, node n_i includes the value $y_i = f_i(0) * P$ in each of these messages.
5) Finally every node has values received from other founding nodes and also it's own value $f_{ii}(h(n_i), z)$ with it. Then every node n_i computes $f_i(z) = f(h(n_i), z) = \sum_{j \in k} f_{ji}(h(n_i), z)$.
6) Now every node ni has partial secret $s_i = f_i(0)$ and a secret equation $f(h(n_i), z)$.
7) The public key of the MANET is $pk = \sum y_i$ for $i=(1\ldots\ldots n)$.

The MANET secret function $f(x, z) = \sum_{j \in k} f_i(x, z)$ and MANET secret key is $s = f(0, 0)$ are safe and hidden.This secret information can only be reconstructed if and only if there are at-least t nodes having partial share of MANET secret. For a new node n_w trying to join the network, it has to request at-least t nodes for the values $f_{iw}(h(n_i), h(n_w))$. When t nodes accept the node n_w request, then they send $f_{iw}(h(n_i), h(n_w))$ to node n_w. Now node n_w has t values and these values are used in Lagrange's interpolation to derive a secret polynomial corresponding to node n_w, Lagrange's interpolation is applied as follows:

$f_w(z) = f(h(n_w), z) = \sum_{nj \in n} \prod_{ni \in n, ni \neq nj} (z - h(n_i))/ (h(n_j) - h(n_i)) * f(h(n_i), h(n_w))$

The partial secret of node n_w is $f_w(0)$ and secret polynomial of node n_w is $f_w(z)$ i.e., $f(h(n_w), z)$

B. Key Generation

After every node n_i has received a partial secret s_i, then the nodes run RSA key generation protocol to generate a public (pk_i) and private (sk_i) key pair. The private key (sk_i) is kept secret with the node n_i and public key (pk_i) is made available to all other nodes. The public key pk_i is used to encrypt messages that are sent to node n_i, and the node n_i uses its private key sk_i to decrypt messages and also to sign.

A threshold number of nodes can sign a certificate. The public key is associated with the node identity in the certificate. This certificate management can be done as in [22].

C. Sub-Group Operations

Every node n_i has a secret univariate polynomial as well as a secret share of the MANET. If t' (for t'<t) nodes want to form a subgroup they run the same protocol as the 'setup'. This is achieved as follows:

1) Every node n_i has a secret univariate polynomial $f(h(n_i), z)$ in degree 't-1'.
2) The nodes that want to form a subgroup eliminate higher order variables greater than t'-1.
3) Every node n_i computes $f_{ij}(h(n_i), h(n_j))$ for remaining nodes of subgroup and itself, $1 \leq i, j \leq t'$.
4) Now every node secretly sends computed $f_{ij}(h(n_i), h(n_j))$ to corresponding node n_j. Furthermore, node n_i includes the value $y_i = f_i(0) * P$ in each of these messages.
5) Finally every node in the subgroup has values received from other nodes and also it's own value $f_{ii}(h(n_i), h(n_i))$ with it.
6) Then every node n_i computes $fi(h(n_i), h(n_j)) = \sum_{(i,j) \varepsilon t'} f_{ji}(h(n_j), h(n_i))$.
7) Now every node n_i has partial secret $s_i' = f_i(h(n_i), h(n_j))$ corresponding to the subgroup.

The public key and secret key corresponding to the subgroup are $pk_{sg} = \sum y_i$ for $i=(1\ldots\ldots t')$. and $s_{i'}$ respectively. The secret shares of subgroup can be used to sign/decrypt subgroup messages, this can be achieved using the protocol in nc kumar et al [22]. Which uses bls signature, that is efficient for resource constraint networks such as MANET.

IV. CONCLUSIONS

In this paper, we proposed a new scheme that performs subgroup operations efficiently in decentralized PKI based MANETS. In our scheme the nodes of the MANET holds a secret share and every node chooses its own public and private keys. Our scheme uses a bivariate polynomial in setting up the MANET in a distributed manner and a univariate polynomial to perform subgroup operations to reduce the communication overhead.

Thus, other interesting and desirable properties for a MANET such as threshold operations involving subgroups of nodes can be implemented and proactive security techniques can be used to support long-lived MANET.

REFERENCES

[1] F. Anjum and P. Mouchtaris, Security for wireless ad hoc networks. Wiley-Blackwell, Mar. 2007.

[2] Vanesa Daza, Javier Herranz, Paz Morillo, Carla Rfols, Cryptographic techniques for mobile ad-hoc networks, Computer Networks, Volume 51, Issue 18, 19 December 2007.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson. Ariadne: A secure on-demand routing protocol for adhoc networks. In Proceedings of the Eighth ACM International Conference on Mobile Computing and Networking (Mobicom 2002), September 2002.

[4] Y.-C. Hu, A. Perrig, and D. B. Johnson. Packet leashes: A defense against wormhole attacks in wireless networks. In Proceedings of IEEE Infocom 2003, April 2003.R. E. Sorace, V. S. Reinhardt, and S. A. Vaughn, “High-speed digital-to-RF converter,” U.S. Patent 5 668 842, Sept. 16, 1997. (2002) The IEEE website. [Online]. Available: http://www.ieee.org/

[5] S. Kent and T. Polk. Public-key infrastructure (x.509) (pkix) charter. http://www.ietf.org/html.charters/pkix-charter.html.

[6] L. Zhou, Z.J. Haas, Securing ad hoc networks, IEEE Network 13 (6) (1999) 24-30.

[7] G.R. Blakley, Safeguarding cryptographic keys, in: Proceed- ings of the National Computer Conference, American Federation of Information, Processing Societies Proceedings, vol. 48, 1979, pp. 313-317.

[8] A. Shamir, How to share a secret, Communications of the ACM 22 (1979) 612-613.

[9] Seung Yi and Robin Kravetso. Moca : Mobile certificate authority for wireless ad hoc networks. In The second anunual PKI research workshop (PKI 03), Gaithersburg, 2003.

[10] Dan Boneh, Ben Lynn, and Hovav Shacham (2004). ”Short Signatures from the Weil Pairing”. Journal of Cryptology. 17: 297-319.

[11] Djenouri, Djamel, L. Khelladi, and N. Badache. ”A survey of security issues in mobile ad hoc networks.” IEEE communications surveys 7.4 (2005): 2-28.

[12] Stallings, William (1990-05-03). Cryptography and Network Security: Principles and Practice. Prentice Hall. p. 165. ISBN 9780138690175.

[13] H. Luo, J. Kong, P. Zerfos, S. Lu, L. Zhang, URSA: ubiquitous and robust access control for mobile ad hoc networks, IEEE/ACM Transactions on Networking 12 (6) (2004).

[14] M. Narasimha, G. Tsudik, J.H. Yi, On the utility of distributed cryptography in P2P and MANETs: the case of membership control, in: Proceeding of ICNP203, 2003, pp. 336-345.

[15] S. Jarecki, N. Saxena, J.H. Yi, An attack on the proactive RSA signature scheme in the URSA ad hoc network access control protocol, in: Proceedings of the SASN04, 2004, pp. 19.

[16] 16. C. Blundo, A. De Santis, A. Herzberg, S. Kutten, U. Vaccaro, M. Yung, Perfectly-secure key distribution for dynamic conferences, in: Proceedings of Crypto92, LNCS, vol. 740, Springer-Verlag, 1993, pp. 471-486.

[17] J. Anzai, N. Matsuzaki, T. Matsumoto, A quick group key distribution scheme with entity revocation, in: Proceedings of Asiacrypt99, LNCS, vol. 1716, Springer-Verlag, 1999, pp. 333-347.

[18] V. Daza, J. Herranz, G. Sez, Constructing general dynamic group key distribution schemes with decentralized user join, in: Proceedings of ACISP03, LNCS, vol. 2727, Springer- Verlag, 2003, pp. 464-475.

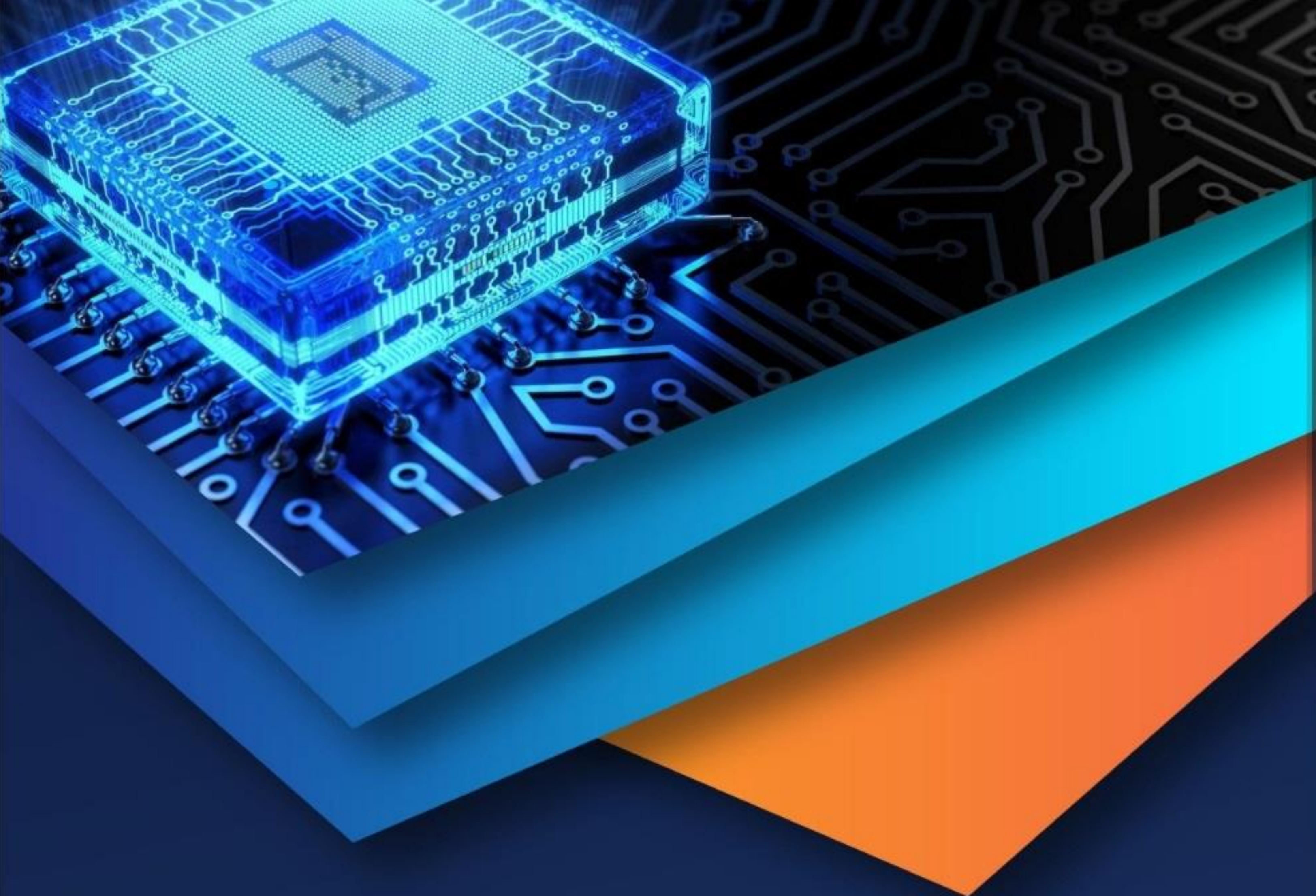
[19] N. Saxena, G. Tsudik, J.H. Yi, Efficient node admission for short-lived mobile ad hoc networks, in: Proceedings of ICNP05, 2005, pp. 269-278.

[20] Daxing Wang, Jikai Tang. ”Efficient Aggregate Signature Algorithm and Its Application in MANET”. in: International Journal of Mathematical, Computational, Physical, Electrical and Computer Engineering. vol. 7, No:11, 2013.

[21] Hanoka G, Shuldt J.C.N, ”On signatures with tight security in the multi-user setting” (2017) in : Proceedings of 2016 International Symposium on Information Theory and Its Applications, ISITA 2016, art. no. 7840392, pp. 91-95.

[22] Kumar, N. C., Basit, A., Singh, P., Venkaiah, V. C., & Rao, Y. V. (2017). Node Authentication Using BLS Signature in Distributed PKI Based MANETs. International Journal of Network Security & Its Applications, 9(4), pp.33-44.

©IJRASET (UGC Approved Journal): All Rights are Reserved



10.22214/IJRASET

INDEX COPERNICUS

45.98

IMPACT FACTOR: 7.129

TOGETHER WE REACH THE GOAL

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)