Source Anonymous Message authentication on Elliptic Curve in Mobile Ad Hoc Network

T.R.Ajey Vignesh[#1],B.Arun Karthikeyan[#2], K.Ramesh[#3] (Assistant Professor)
[#12]PG Department of Embedded Systems and Technologies,[#3] Department of Computer Applications
Regional Centre of Anna University,Tirunelveli
[#1]ajey_vignesh@yahoo.co.in
[#3]ramesh7n@yahoo.co.in

Abstract : - Security and protection of private user information are a prerequisite for the deployment of the mobile network technologies. However, the establishment of secure communication architecture within mobile ad hoc networks encounter special challenges, due to the trait and specific cities of such environment. A number of secure authentication schemes based on asymmetric cryptography have been proposed to prevent such attacks. In this paper, security of private user information is provided by a hybrid technology, merging SAMAC (Source Anonymous Message Authentication Code) with Elliptical curve cry topography algorithm. Using this interesting issues arising in such MANETs by designing an anonymous routing framework (ALERT) extended to key server management and digital signature algorithm. It uses nodes' current locations to construct a secure MANET. Based on the current location, each node can decide which other relay nodes it wants to communicate with.

Keywords: Modified Elgamal Signature (MES), Source Anonymous Message Authentication Code (SAMAC)

I Introduction

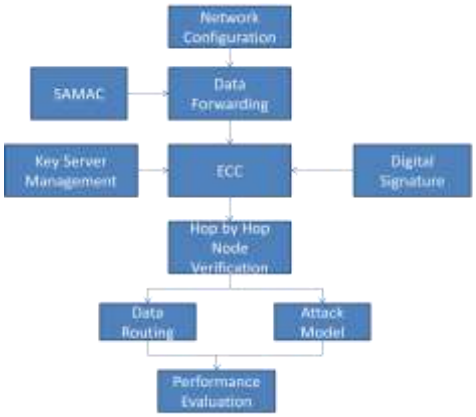
Rapid development of Mobile Ad Hoc Networks (MANETs) has stimulated numerous wireless applications that can be used in a wide number of areas such as commerce, emergency services, military, education, and entertainment. MANETs feature self-organizing and independent infrastructures, which make them an ideal choice for uses such as communication and information sharing. Because of the openness and decentralization features of MANETs, it is usually not desirable to constrain the membership of the nodes in the network. Nodes in MANETs are vulnerable to malicious entities that aim to tamper and analyze data and traffic analysis by communication eavesdropping or attacking routing protocols. Although anonymity may not be a requirement in civil oriented applications, it is critical in military applications (e.g., soldier communication). Consider a MANET deployed in a battlefield. Through traffic analysis, enemies may intercept transmitted packets, track our soldiers (i.e., nodes), attack the commander nodes, and block the data transmission by comprising relay nodes (RN), thus putting us at a tactical disadvantage.

We propose an unconditionally secure and efficient source anonymous message authentication scheme (SAMAC). The main idea is that for each message *m* to be released, the message sender, or the sending node, generates a source anonymous message authenticator for the message *m*. The generation is based on the MES scheme on elliptic curves. For a ring signature, each ring member is required to compute a forgery signature for all other members in the AS. In our scheme, the entire SAMAC generation requires only three steps, which link all non-senders and the message sender to the SAMAC alike. In addition, our

design enables the SAMAC to be verified through a single equation without individually verifying the signatures.

II Proposed Work

A.System Model



B. Proposed MES Scheme on Elliptic Curves

Let $p > 3$ be an odd prime. An elliptic curve E is defined by an equation of the form:

$E : y2 = x3 + ax + b \bmod p$, where $a, b \in Fp$, and $4a3 + 27b2 \_\equiv 0 \bmod p$. The set $E(Fp)$ consists of all points $(x, y) \in Fp$ on the curve, together with a special point O, called the point at infinity.

Let $G = (xG, yG)$ be a base point on $E(Fp)$ whose order is a very large value N. User A selects a random integer $dA \in [1, N - 1]$ as his private key. Then, he can compute his public key QA from $QA = dA \times G$.

Signature generation algorithm:

For Alice to sign a message m, she follows these steps:

1) Select a random integer kA, $1 \le kA \le N - 1$.

2) Calculate $r = xA \bmod N$, where $(xA, yA) = kAG$. If $r = 0$, go back to step 1.

3) Calculate $hA \leftarrow^{l} h(m, r)$, where h is a cryptographic hash function, such as SHA-1, and $\leftarrow^{l}$ denotes the l leftmost bits of the hash.

4) Calculate $s = rdAhA + kA \bmod N$. If $s = 0$, go back to step 2.

5) The signature is the pair (r, s).

Signature verification algorithm:

For Bob to authenticate Alice's signature, he must have a copy of her public key QA, then he:

1) Checks that $QA \_= O$, otherwise invalid

2) Checks that QA lies on the curve

3) Checks that $nQA = O$

After that, Bob follows these steps to verify the signature:

1) Verify that r and s are integers in $[1, N - 1]$. If not, the signature is invalid.

2) Calculate $hA \leftarrow^{l} h(m, r)$, where h is the same function used in the signature generation.

3) Calculate $(x1, x2) = sG - rhAQA \bmod N$.

4) The signature is valid if $r = x1 \bmod N$, invalid otherwise.

In fact, if the signature is correctly generated, then:

$(x1, x2) = sG - rhAQA$

$= (rdAhA + kA)G - rhAQA$

$= kAG + rhAQA - rhAQA$

$= kAG.$

Therefore, we have $x1 = r$, and the verifier should Accept the signature.

Suppose that the message sender (say Alice) wishes totransmit a message m anonymously from her network node toany other nodes. The AS includes n members, $A1, A2, \cdots, An$.

e.g., $S = \{A1, A2, \cdots, An\}$, where the actual message senderAlice is At, for some value t, $1 \le t \le n$. In this paper, wewill not distinguish between the node Ai and its public keyQi. Therefore, we also have $S = \{Q1, Q2, \cdots, Qn\}$.

Authentication generation algorithm:

Suppose m is amessage to be transmitted. The private key of the messagesender Alice is dt, $1 \le t \le N$. To generate an efficient SAMACfor message m, Alice performs the following three steps:

1) Select a random and pairwise different *ki* for each 1 ≤*i* ≤ *n* − 1, *i* _= *t* and compute *ri* from (*ri, yi*) = *kiG*.
2) Choose a random *ki* ∈*Zp* and compute *rt* from (*rt, yt*) =*ktG*$\sum_{i\neq t} rihiQi$such that *rt* ≠0 and *rt* ≠*ri* for any*i* ≠*t,* where *hi*←^{l}*h*(*m, ri*).
3) Compute *s* = *kt* + $\sum_{i\neq t} k_{l}$+*rtdtht* mod *N*.

The SAMAC of the message *m* is defined as:
S(*m*) = (*m, S, r*1, *y*1, ・ ・ ・, *rn, yn, s*).

Verification algorithm:
For Bob to verify an alleged
SAMAC (*m, S, r*1, *y*1, ・ ・ ・, *rn, yn, s*), he must have a copy of
the public keys *Q*1, ・ ・ ・,*Qn*. Then he:
1) Checks that *Qi* _= *O, i* = 1, ・ ・ ・, *n*, otherwise invalid
2) Checks that *Qi, i* = 1, ・ ・ ・, *n* lies on the curve
3) Checks that *nQi* = *O, i* = 1, ・ ・ ・, *n*
After that, Bob follows these steps:
1) Verify that *ri, yi, i* = 1, ・ ・ ・, *n* and *s* are integers in[1,*N* − 1]. If not, the signature is invalid.
2) Calculate *hi*←^{l}*h*(*m, ri*), where *h* is the same function used in the signature generation.
3) Calculate (*x*0, *y*0) = *sG* –$\sum_{i=1}^{n} rihiQi$
4) The signature is valid if the first coordinate of$\sum_{i} xiyi$ equals *x*0, invalid otherwise.

In fact, if the SAMAC has been correctly generated withoutbeing modified, then we compute:
(*x*0, *y*0) = *sG* –$\sum_{i=1}^{n} rihiQi$
= (*kt* +$\sum_{i\neq t} ki$+ *rtdtht*)*G* –$\sum_{i} rihiQi$
= $\sum_{i\neq t} kiG$+ (*ktG* - $\sum_{i\neq t} rihiQi$)
= $\sum_{i\neq t} riyi$ + (*rt, yt*)
= $\sum_{i} riyi$
Therefore, the verifier should always Accept the SAMAC.
Remark 1. *It is apparent that when n* = 1, *SAMAC becomes asimple signature algorithm.*

III Security Analysis

In this subsection, we will prove that the proposed SAMAC scheme can provide unconditional source anonymity and provable unforgeability against adaptive chosen-message attacks.

1) Anonymity: In order to prove that the proposed SAMACcan ensure unconditional source anonymity, we have to provethat: (i) for anybody other than the members of *S*, the probabilityto successfully identify the real sender is 1*/n*, and (ii)anybody from *S* can generate SAMACs.

2) Unforgeability: The design of the proposed SAMAC relieson the ElGamal signature scheme. Signature schemes canachieve different levels of security. Security against existentialforgery under adaptive-chosen message attacks is the maximumlevel of security.In this section, we will prove that the proposed SAMACis secure against existential forgery under adaptive-chosenmessage attacks in the random oracle model [21]. The securityof our result is based on elliptic curve cryptography (ECC),which assumes that the computation of discrete logarithms onelliptic curves is computationally infeasible. In other words, no efficient algorithms are known for non-quantum computers. Therefore, we can compute the elliptic curve discrete logarithmof *Qj* in base *G* with non-negligible probability, whichcontradicts the assumption that it is computationally infeasibleto compute the elliptic discrete logarithm of *Qj* in base *G*.Therefore, it is computationally infeasible for any adversary toforge a valid SAMAC.

IV Results

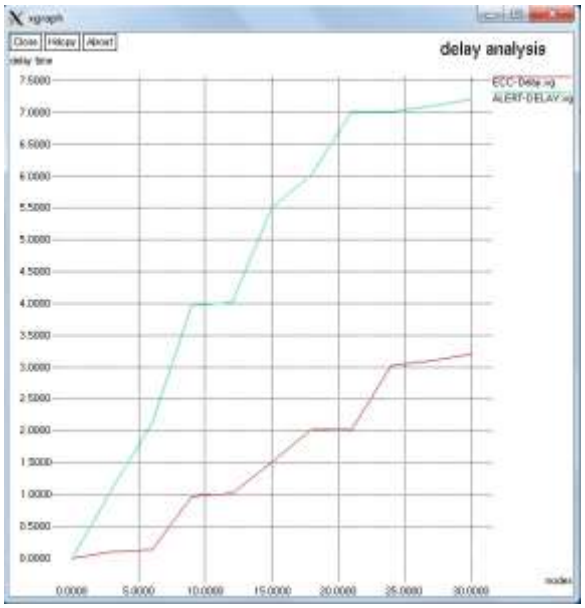


Fig. 1 Delay Analysis

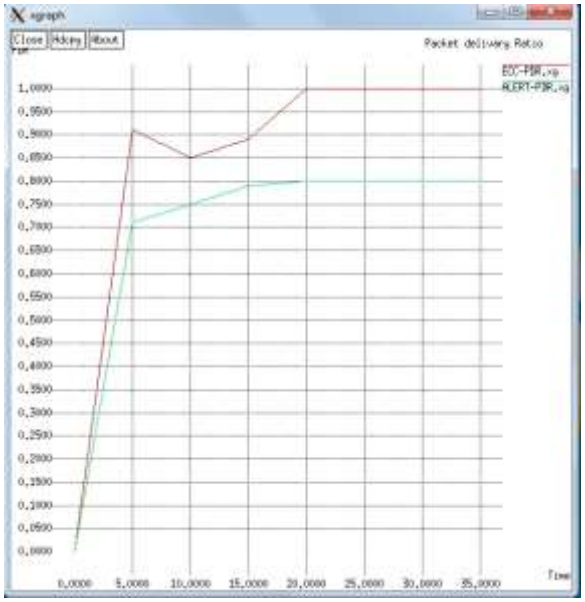


Fig.2 Packet Delivery Ratio

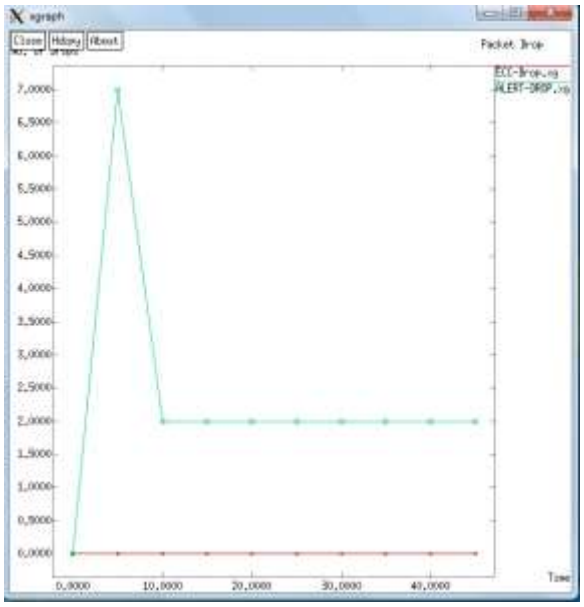


Fig.3 Packet Drop

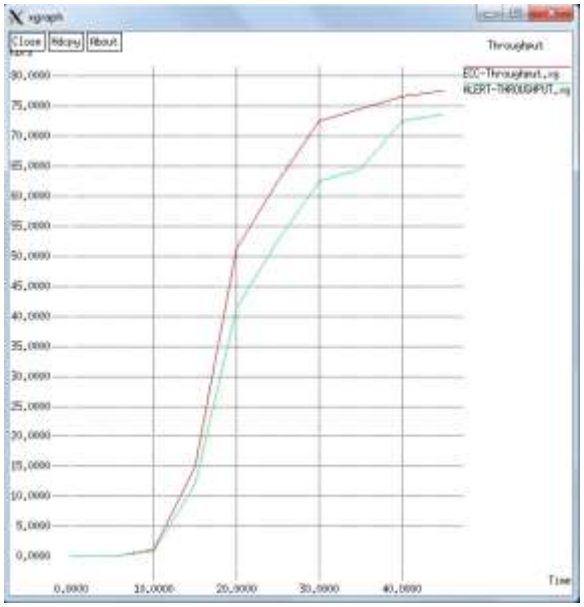


Fig.4 Throughput

V Conclusion

Message authentication has always been a major threat to the security in wireless sensor Networks. A Novel and efficient source anonymous message authentication scheme based on ECC to provide message content authenticity. To provide hop by hop message authentication without the weakness of the built in threshold of the polynomial based scheme. SAMAC based on ECC compared it against other popular mechanisms in different scenarios through simulations and TelosB. Simulations results indicate that it

greatly increases the effort of an attacker, but it requires proper models for every application. Proposed scheme is more efficient than the bivariate polynomial-based scheme in terms of computational overhead, energy consumption, delivery ratio, message delay, and memory consumption.

References

[1] L. Zhao and H. Shen, "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE TRANS On Mobile Computing, Vol. 12, No. 6, June 2013.

[2] C.-C. Chou, D.S.L. Wei, C.-C. Jay Kuo, and K. Naik, "An Efficient Anonymous Communication Protocol for Peer-to-Peer Applications over Mobile Ad-Hoc Networks," IEEE J. Selected Areas in Comm., vol. 25, no. 1, pp. 192-203, Jan. 2007.

[3] Y. Zhang, W. Liu, and W. Luo, "Anonymous Communications in Mobile Ad Hoc Networks," Proc. IEEE INFOCOM, 2005.

[4] J. Kong, X. Hong, and M. Gerla, "ANODR: Anonymous on Demand Routing Protocol with Untraceable Routes for Mobile Ad-Hoc Networks," Proc. ACM MobiHoc, pp. 291-302, 2003.

[5] Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA), 2002.

[6] I. Aad, C. Castelluccia, and J. Hubaux, "Packet Coding for Strong Anonymity in Ad Hoc Networks," Proc. Securecomm and Workshops, 2006.

[7] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering false data in sensor networks," in IEEE Symposium on Security and Privacy, 2004.

[8] H. Wang, S. Sheng, C. Tan, and Q. Li, "Comparing symmetric-key and public-key based security schemes in sensor networks: A case study of user access control," in IEEE ICDCS, Beijing, China, 2008, pp. 11–18.

[9] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems," Communications. of the Assoc. of Comp. Mach., vol. 21, no. 2, pp. 120–126, 1998.