International Journal of Applied Engineering Research ISSN 0973-4562 Volume 10, Number 14 (2015) pp 34726-34732

An Improved Privacy Tackled Hybrid Elliptic Arc Digital Autograph Algorithm (EADAA) in VANETs for Secure Communication

[1] Prof.C.Thangamalar [2] Dr.K.Ravikumar
[1]Research and Development Centre, Bharathiar University, Coimbatore 641046.
[2]Assistant Professor, Dept.of.Computer science, Tamil University Thanjavur, India

Abstract- In This paper, A safe and well-organized procedure in favor of vehicular Ad hoc network contain be projected as a result because toward ensures together memo confirmation and solitude preservation. similar toward security linked memo might contain life serious information, It is A necessity as a result because toward the dispatcher similar toward fine similar toward the memo be authentic. The projected method is base going on A safe elliptic arc digital autograph algorithm approach. The projected method supports restricted privacy, anywhere the user's site be able toward be revealed next toward the willingness of the user.separately beginning this, the method is safe not in favor of attack similar toward DoS, Sybil and Grey/Black gap attacks. beginning the judgment because A result of previous toward projected schemes, It is found as a result because toward the projected method similar toward base going on elliptic arc separate logarithmic problem, outperforms toward be had algorithms base going on numeral factoring and separate logarithmic problem.

Index Terms- VANETs, Authenticity, Privacy, Anonymity, EADAA.

1. Introduction

Vehicular Ad hoc network (VANET) be able toward be define similar toward A structure of cell phone Ad hoc network (MANET) toward give connections among close by automobile and among automobile and close by put edge equipments. inside additional words, VANET is A technology as a result because toward uses moving automobile similar toward nodes inside A method toward build A cell phone network. It turns every participate automobile mixed up in A wireless router otherwise node, allow automobile roughly 100 toward 300 meters of every additional toward connect and, inside turn, build A method because A result of A wide range. similar toward automobile fall not in of the signal collection and drop not in of the network, additional automobile be able toward connect in, connecting automobile toward single one extra as a result therefore because toward A cell phone Internet is created. Inside order toward connect the method every automobile passes from side toward side A series of registration and confirmation phases.

VANETs be A hopeful move toward in favor of facilitating intelligent transportation method (ITS) as a result because toward includes highway safety, move management, and infotainment dissemination in favor of drivers and passengers. securities A fundamental matter in favor of hopeful applications inside such networks. Due toward extraordinarily high mobility of automobile inside A vehicular network, repeated give up requests will be A norm, which initiates the demand in favor of an effective and fast confirmation method as a result because toward be able toward keep the repair continuity inside attendance of the repeated give up events. This imposes the need in favor of A strong memo confirmation method as a result because toward guarantee confirmation similar toward fine similar toward integrity. Also, VANETs be extremely vulnerable toward solitude threats. inside A VANET, an opponent be able toward easily monitor several target vehicle, track its site and extract in order as a result because toward is confidential and secret toward as a result because toward vehicle. Therefore, one extra important security requirement of VANETs is toward preserve the solitude of the participate nodes. Thus, the ultimate aim of the security solutions in favor of VANETs is toward give security services, such similar toward authentication, confidentiality, integrity, privacy, anonymity, and availability, toward the users. separately beginning these, VANETs be prone toward a few specific attack such similar toward the Denial of repair (DoS) attacks, Sybil attacks, Grey gap attacks, Black gap attack and as a result on.

The projected method is base going on elliptic arc digital autograph algorithm (EADAA) which generates safe signature as a result because toward be toward be create use of because A result of the participate nodes. The automobile be provided because A result of short-term identity as a result because toward be produce create use of safe cryptographic techniques. These short-term identity be create use of during several sort of communication, thereby preserving solitude and give secrecy toward the user. This method facilitates methods toward prevent Sybil attack and presents method toward notice DoS attacks, Grey gap attack and Black gap attacks.

The remaining sections of this article is organized similar toward follows. part 2 provide the linked workings in favor of safe VANET exist inside literature. The projected method in favor of A safe and well-organized VANET is discuss inside part 3.part 4 describes the presentation matter of the projected scheme. Finally, part 5 discusses the concluding remarks.

2. Toward be had workings linked toward safe VANETS

The fundamental objective of a safe VANET is toward facilitate safe memo inside an opponent environment. in favor of instance, condition two parties, A and *B*, wish for toward safely converse above an energetic network, they would definitely wish for toward create sure as a result

because toward the in order they correspond among themselves must remain secret and authenticity of the in order must be maintained. present contain be A numerous studies perform because A result of researchers toward obtain These security aim and give A safe and friendly surroundings toward the user of the vehicular network. These documents be base going on the a variety of type of cryptosystems available.

2.1. Protocol in favor of memo confirmation and solitude Preservation

Message confirmation because A result of solitude maintenance is A very energetic topic in favor of securing VANETs. The idea of Identity based secrecy approach is toward create automobile not identifiable. According toward Rongxing [1], present be two fundamental models in favor of identity-based secrecy approaches: single is huge unidentified key base (HAB) [2], [1], [3], the additional is collection autograph method base (GSB) [4], [5].together of them be able toward lecture toward the security necessities well, such similar toward authentication, non-repudiation, individuality revocation, and restricted anonymity. Inside the group-signature-based schemes, utilizing collection signature [6], several open entity will not reveal the originator individuality of A routine move memo [7], [8]. However, single limitation is as a result because toward the price in favor of sign and verifying mail is far extra than adopting the conventional public-key base signature. toward reduce These overheads, A. Wasef et al. [9] propose the Hybrid scheme, wherein A automobile be able toward matter A permit in favor of itself because A result of create use of A collection answer and later than that sign its mail create use of the public key-based signature. inside such A way, the average above your head of memo confirmation be able toward decrease. This method achieve A trade off among the group-signature-based method and conventional PKI-based schemes.

However, due toward the narrow bandwidth of wireless memo and the high-speed mobility of vehicles, It is difficult toward distribute A big permit revocation list (CRL) toward each and every single automobile inside A timely fashion. toward reduce the CRL size, Bellur [7] suggests segmenting A country mixed up in A quantity of geographic regions and assigning region-specific permit because A result of A strength time toward A vehicle. Lu et al. [1] develop the well-organized restricted solitude maintenance (ECPP) protocol, which is the primary procedure toward support legitimate automobile updating short occasion Pseudonymous permit beginning the RSUs frequently.

2.1.1. Method base going on sightless autograph and One-Way mess Function.

The method because A result of Chun-Ta Li et al. [10]not single accomplishes V2V and V2I confirmation and answer establishment in favor of memo among members, except in addition integrates sightless autograph method mixed up in the method inside allow cell phone automobile toward namelessly act together because A result of the military of edge infrastructure. According toward the security fear and solitude matter mixed up in consideration, the method claim toward keep essential requirements.

2.1.2. Memo confirmation method base going on EADAA

EADAA is A variant of the digital autograph algorithm (DSA) as a result because toward operates going on elliptic arc groups [11]. S. S. Manvi et al. inside [12], projected an well-organized memo confirmation method as a result because toward is base going on elliptic arc digital autograph algorithm (EADAA). The authors of the article contain claimed toward overcome a few intrinsic drawback of toward be had authenticate and security method like: extra dealing out wait in favor of confirmation next toward dispatcher and receiver, Computational and communicational overheads, storage space requirements, etc.

2.2. Intrinsic drawback of toward be had Schemes

The toward be had method be well-organized and reliable. The researchers contain in addition prove their claim toward be right and up toward mark. Every of These documents contain significant contributions toward the security of VANETs. a few of These intrinsic drawback of the toward be had method be listed below:

- More dealing out wait in favor of confirmation next toward dispatcher and receiver.
- Computational and Communicational overheads. List of revoked automobile have toward be continuously modernized and broadcasted toward each and every single nodes, This leads toward Computational complexities.
- Storage/memory necessities in favor of storing the modernized revocation lists similar toward fine similar toward every pseudonym need toward be certified and stored.

Motivated because A result of this, A procedure contain be projected as a result because toward takes the advantages of the toward be had method and improves them as a result similar toward to obtain authentication, restricted solitude and security not in favor of attacks. The method provide in order integrity, in order origin authentication, non-repudiation, reliability and efficiency. It is base going on EADAA similar toward A 160-bit answer inside ECC is similar toward secured similar toward 1024-bit answer inside RSA and, ECC is sooner and occupies fewer recall space. in addition It guarantee security similar toward ECDLP is extra safe similar toward evaluate toward its counterparts IFP and DLP.

3. Projected method in favor of safe VANET

3.1. Method model

Some plan decision be completed inside the course of building the method model. These decision be completed later than taking mixed up in concern together practical implementation and presentation issues.

Let us consider A VANET composed of A big quantity of automobile V = $\{V_1,V_2,...\}$ and A spot of edge units (RSUs) $R = \{R_1,R_2,...\}$, similar toward exposed inside Figure 4.1 [13]. inside the VANET, every vehicle$V_i \in V$ contain A unique nonzero identifier and move beginning single position toward one extra either along A put route (e.g., bus) otherwise because A

result of choosing A dynamical path (e.g., taxi), while every RSU $R_j \in R$ is placed next toward a few serious locations $L_{j\ inside}$ the area. The connections among automobile and automobile be bidirectional, i.e., two automobile inside the broadcast collection $T_{V\ be\ able\ toward\ converse}$ because A result of every other. However, because RSU's broadcast collection TR is larger than T_V , the memo among automobile and RSU is not entirely bidirectional. Assume as a result because toward the distance among automobile $V_i$and RSU $R_j$is d = $|V_i - R_j|$.while$T_V < d \leq T_R$, single $V_{i\ be\ able\ toward\ notice}$ the existence of R_j; while $0 \leq d \leq T_V$, V_i and $R_{j\ be\ able\ toward\ converse}$ because A result of every other.

3.2. The projected Protocol

In This section, an RSU aided memo confirmation method contain be projected which shall in addition give restricted solitude preservation. While A automobile shall come inside the collection of an RSU, It shall call for the RSU in favor of A short-term identification known similar toward pretend identification which will be valid twist over the automobile move toward one extra RSU's range. This pretend identification will be create use of because A result of the dispatcher automobile in favor of its individuality instead of its real identity. while the automobile needs toward launch A message, the automobile shall mark the memo because A result of its secret answer create use of EADAA autograph and append its short-term identification inside position of dispatcher address. The automobile which receive the memo shall query the RSU in favor of the open answer of the dispatcher automobile and provide the sender's pretend identification inside the request. The RSU shall find not in the real identification beginning the pretend identification and transmit the matching open answer of the dispatcher vehicle. The mixed up automobile shall confirm the dispatcher automobile autograph and therefore authenticate the memo except the sender's individuality remains unidentified toward the getting vehicles.

Notations as a result because toward be create use of throughout This projected method be summarized inside bench 1 and the information of the projected method be described inside the next subsections.

3.2.1. Automobile registration because A result of Trusted Authority. previous toward

VANET setup, mixed up automobile shall list themselves because A result of transportation authorities. This will be an offline process. The automobile proprietor shall give its identity, lecture toward and proof in favor of the same. later than verification, the transportation power shall ask the proprietor toward give the answer pond toward be registered. The automobile proprietor shall produce A pond of EADAA public-private answer pairs create use of next algorithm.

A automobile A's answer pair is associated because A result of A particular put of EC area parameter d = (q,F_R,a,b,G,n,h).

Table 1. Notations create use of from side toward side The Proposed Scheme

Symbols Used	Description
Qi, di	Public and secret answer ofithvehicle
TID_i	Temporary identification ofithvehicle
VID_i	Actual identification ofithvehicle
S	Source
D	Destination
RSU_{Pr}	Private answer of RSU
$H(m)$	A cryptographic mess purpose going on memo m
$\oplus$	Exclusive-Or operation
TD	Timestamp, as a result because toward end attaches
TS	Timestamp, as a result because toward cause attaches
$a\|\|b$	Concatenation of A and b
TID_S, TID_I, TID_D	Temporary identification of Source, middle and end automobile resp.
D	Elliptic arc area parameter
M_i	Message sent inside ithiteration
ACK_j	Acknowledgement inside j^{th}iteration

This association is certain cryptographically i.e. from side toward side certificates.

Pick A chance otherwise pseudorandom numeral d *inside* the interval [1,n − 1].

Calculate QA = d ∗ G.

A's open answer is QA and secret answer is d.

in favor of dissimilar principles of d, dissimilar QA principles be produce which shall structure the pond of open key in favor of automobile A.

Vehicle A shall list These open key not in favor of its identification which is V ID_A. These open key contain A certain strength period. later than the strength time expires, A have toward renew the open answer pond because A result of generating and registering A fresh put of open keys. The transportation power later than that matter permit authenticate the open keys.in favor of This It signs the permit because A result of its secret key. Several third party be able toward authenticate These permit create use of the open answer of the TA.

3.2.2. RSU Installation Phase. later than automobile registered, the transportation power shall deploy RSUs next toward every highway section. It shall upload the information of the entire automobile list twist over date toward the RSU. inside twist the RSU in addition will be list because A result of the TA and its open answer shall be convey toward each and every single the list vehicles.

Temporary individuality Acquisition Phase. While

A vehicle's collection reaches an RSU, the automobile launch A call for toward the RSU toward give A short-term identity. It in addition launch its individuality and open answer permit which It shall create use of inside further communication. The RSU shall authenticate the individuality

and the permit in favor of the open key. later than that It shall produce A short-term individuality in favor of the automobile and launch It inside the reply.

TID_I = V IDI $\oplus(RSU_{Pr})$ (1)

Message remove Phase.

The memo remove perform because A result of the automobile inside A VANET be able toward be broadly categorized mixed up in two types.

A. Transmit of Message.

- **Step I: sign the Messages**

When the automobile needs toward launch A memo primary It needs toward mark the memo because A result of its secret answer matching toward the open answer It contain convey toward the RSU. It shall not launch its right identity. Instead It shall create use of its short-term individuality TID.

- **Step II: open answer Look Up** The automobile which receive the memo and the autograph shall enquire the close by RSU in favor of the open answer matching toward the TID_I. The RSU shall calculate V IDI $_{beginning}$ the TIDI similar toward follows:

V IDI = TIDI $\oplus(RSU_{Pr})$ (2)

Then It shall retrieve the open answer in favor of the V IDI and transmit it. The mixed up automobile shall create use of the open answer in favor of confirmation of the memo received. **.** walk **III: memo autograph confirmation** The automobile later than getting the open key, shall confirm the autograph going on the memo create use of EADAA autograph confirmation method discuss earlier.

B. Personalized memo Transfer.

The whole procedure is divided mixed up in two steps, such as: Firstly, checking of the attendance of end automobile inside the collection of RSU, and secondly, the memo process. present might arise 2 belongings inside the above said memo process.

a. Destination is inside the collection of together cause and RSU.
b. Destination is not inside the collection of cause except is inside the collection of RSU.

1. Checking of the attendance of end automobile inside the collection of RSU. inside This walk the cause automobile check whether the end automobile is current inside the collection of RSU otherwise not. **.** walk **1:** The cause automobile launch the short-term individuality (TID_S) assigned toward It and short-term individuality of end vehicle(TID_D) toward the RSU inside its range.

- **Step 2: later than** getting the short-term identities, the concerned RSU check its possess database toward confirm whether the end automobile is current inside it's collection otherwise not.
- **Step 3: condition** the end automobile is current inside the collection of RSU, later than that as a result because toward RSU launch A optimistic acknowledgement (ACK) toward the cause vehicle; otherwise It launch A unenthusiastic acknowledgement (NACK).
- **Step 4: condition unenthusiastic** acknowledgement comes beginning RSU, later than that the memo procedure stops. condition present is optimistic acknowledgement beginning RSU, later than that the memo procedure begins.

2. Memo process. Prior memo procedure starts, present be a few computations done because A result of cause vehicle. cause automobile primary selects A chance quantity '*a*'. It calculate C = $(Q^2_D)^{H(TS)_* dS\ anywhere}$ Q_D is the open answer of end and Sis the secret answer of the source. TS is the Timestamp produce because A result of the cause vehicle. later than that It calculate C $\oplus$ *a*. According toward the position of attendance of end automobile present be two cases. Together of the belongings will be discuss separately.

Case I: end is inside the collection of together cause and RSU. inside This case, the end automobile is current inside the collection of together cause and RSU.

- **Step 5:** The cause automobile launch the TID_S, TID_D, T_S, C $\oplus$*a toward* end vehicle. later than that C is designed because A result of the cause automobile before.
- **Step 6: next toward primary** the end automobile check whether the recognized short-term end identification is his possess otherwise not. condition It does not competition later than that the memo is dropped. condition It match later than that the end automobile calculate $C' = (Q^2_S)^{H(TS)\oplus dD\ anywhere\ QS}$ and $dD_{be\ open}$ answer of cause and secret answer of end respectively. later than calculate *C*, It recover the chance quantity '*a*' because A result of calculate $C \oplus a \oplus C'$.later than that It will pick A chance quantity '*b*'. later than that It calculate k = *H*(*a*||*b*||0).
- **Step 7:** The end automobile launch TID_D, TID_S, T_D, $C' \oplus (b||k)$ toward the cause vehicle.
- **Step 8:** The cause automobile contain previous toward compute *C*.

Now the cause automobile recover B and k *because A result of* computing $C' \oplus (b||K) \oplus C$.later than that the cause automobile compute $k' = H(a||b||0)$.later than that It evaluate k *because A result of k*. condition together be equivalent toward every additional later than that the end automobile is prove similar toward authentic and joint confirmation obtain recognized among cause and destination.

- **Step 9: later than authenticate** every additional memo remove start among cause and destination. The cause automobile launch TID_S, TID_D, T_S, C $\oplus$Mi toward the end automobile anywhere Miis the memo transfer next toward ithiteration. The end automobile recover the memo Mi because $_{A\ result\ of}$ computing$C' \oplus M_i \oplus C$.
- **Step 10: later than improving** the memo the end automobile launch an acknowledgement toward the cause vehicle.

SoItsends TID_S, TID_D, T_D, $C' \oplus ACK_j$ toward the cause vehicle. The cause automobile recover ACKj *because A result of* computing$C' \oplus ACK_j \oplus C$.

Case II: end is not inside the collection of cause except is inside the collection of RSU. inside This folder the end automobile is not current inside the collection of cause except

It is current inside the collection of RSU. The detail procedure is exposed inside the figure 7 and explained inside a variety of steps.

- **Step 5: similar toward** the end automobile is not current inside the collection of cause vehicle, the cause automobile launch TID_S, TID_D, T_S, C ⊕A toward each and every single the automobile as a result because toward be current inside the collection of source. The C is designed because A result of the cause automobile before.
- **Step 6: inside This** step, each and every single the middle automobile who got the memo beginning the cause automobile check as a result because toward whether the end automobile is current inside their range. several of them who finds the end inside his range, forward TID_S, TID_V , TID_D, T_S, C ⊕A toward the end vehicle.
- **Step 7: next toward primary** the end automobile check whether the recognized short-term end identification is his possess otherwise not. condition It doesn't competition later than that the memo is dropped. condition It match later than that the end automobile calculate $C' = (Q^2_S)^{H(TS)_* dD\ anywhere\ QS}$ and $dD_{be\ open}$ answer of cause and secret answer of end respectively. later than calculate *C*, It recover the chance quantity '*a*' because A result of computing$C \oplus a \oplus C'$ .later than that It will pick A chance quantity '*b*'.later than that It calculate k = *H*(*a*||*b*||0).
- **Step 8:** The end automobile launch TID_D, TID_I, TID_S, T_D, $C' \oplus (b||k)$ toward the middle vehicle.
- **Step 9:** The middle automobile forward TID_D, TID_I, TID_S, T_D, $C' \oplus (b||k)$ toward the cause vehicle.
- **Step 10:** The cause automobile contain previous toward compute *C*. at the present the cause automobile recover B and k *because A result of* computing $C' \oplus (b||K) \oplus C$ .later than that the cause automobile compute $k' = H(a||b||0)$ .later than that It evaluate k *because A result of k*.

If together be equivalent toward every additional later than that the end automobile is prove similar toward authentic and joint confirmation obtain recognized among cause and destination.

- **Step 11: later than authenticate** every additional memo remove start among cause and destination. The cause automobile launch TID_S, TID_D, T_S, C ⊕Mi toward the end automobile anywhere Miis the memo transfer next toward ithiteration.
- **Step 12:** The middle automobile forward TID_S, TID_I, TID_D, T_S, C ⊕Mi toward the cause vehicle. The end automobile recover the memo Mi because *A result of* computing$C' \oplus M_i \oplus C$.
- **Step 13: later than improving** the memo the end automobile launch an acknowledgement toward the intermediate vehicle. as a result It sends TID_D, TID_I, TID_S, T_D, $C' \oplus ACK_j$ *toward* the end vehicle.
- **Step 14:** The middle automobile forward TID_D, TID_I, TID_S, T_D, $C' \oplus ACK_j$ toward the cause vehicle. The cause automobile recover ACKj *because A result of* computing

$C' \quad ACK \quad C$
$\oplus \quad j \oplus \quad .$

Finally, later than completing each and every single These above given ladder of the projected protocol, every automobile inside A VANET be able toward at the present be guaranteed A a lot extra safe driving similar toward fine similar toward communicate environment, because A result of certain solitude preservation.

4. Presentation Analysis

In This section, the presentation of the projected method is evaluated and evaluate because A result of additional linked workings inside conditions bench 2.competence comparisons among the projected method and additional linked schemes of Computational costs. inside[14], He et al. projected an official unidentified ID-based scheme. The security of their method is base going on sightless autograph and RSA cryptosystem. Later, inside [15], Yang et al. projected A safe method in favor of providing unidentified connections inside wireless system without create use of asymmetric cryptosystems. The results of A judgment of competence among the projected scheme, Chun-Ta Li et al.'s method [10], Yang et al.'s method [15] and He et al.'s method [14] be exposed inside bench 2.in favor of evaluation of performance, a few Computational parameter be define similar toward follows.

- T_{exp}— denote the occasion in favor of the modular exponentiation.
- T_{hash}— denote the occasion in favor of the hash operation.
- T_{sym}— denote the occasion in favor of the symmetric encryption/decryption operation.
- T_{asym}— denote the occasion in favor of the asymmetric encryption/decryption operation.
- T_{xor}— denote the occasion in favor of the XOR (⊕) operation.

Parameter	Proposed Scheme	ChunTa-Li's scheme [10]	Yang et al.'s scheme [15]	He et al.'s scheme [14]
Tasym	2	5	0	6
Tsym	0	0	8	2
Texp	0	0	17	0
Thash	4	9	0	5
Txor	9	9	4	0
Total totaling costs	200 *Tsym*	500 *Tsym*	1028 *Tsym*	602 *Tsym*

For instance, A symmetric encryption/decryption is next toward least 100 times sooner than an asymmetric encryption/decryption inside software and an exponential process is roughly equivalent toward 60 symmetric encryptions/decryptions. Moreover, Itrequires 0.0005s toward do A one-way hash process and 0.0087s toward do A symmetric encryption/decryption.

4.1. Computational Overhead

From bench 2, the projected procedure outperforms the additional three toward be had protocols. The Computational expenses of the oneway mess purpose and the XOR (⊕) operation is ignored because These two kinds of operation be quite lighter inside conditions of load than as a result because toward of A symmetric encryption/decryption.

4.2. Memo Overhead

Any two communicate nodes inside the repair phase of the projected method need two memo round toward accomplish joint confirmation and memo integrity. Note as a result because toward two round is the minimum quantity needed in favor of several authentic memo method because A result of joint confirmation toward fulfill its goal.similar toward A result, the projected method is extremely well-organized inside narrow totaling and memo resource environments toward access the dynamic and remote in order systems.

4.3. Storage space Overhead

In the authorization phase, the projected method achieve small storage space expenses because the repair provider (that is the RSU inside This scheme) does not need toward keep official permit per customer next toward each and every single point of occasion and every permit is still safe not in favor of malicious attacks. Inside addition, every customer single needs toward store its possess permit similar toward its permit Certi and its secret key. While the additional repair phase be running, in favor of mixed up participants, including the vehicular joint and the edge unit single need toward keep single permit Certi and two chance numbers (a, b) in favor of every currently in-use permit and therefore the storage space above your head of MAPWPP method is a lot fewer evaluate toward additional linked schemes.

5. Conclusion

In This paper, attempts contain be completed toward plan A safe and well-organized memo method in favor of VANETs. Here A novel RSU mixed up memo method is proposed. similar toward ECDLP is create use of in favor of encryption, hence the protocol need fewer Computational power, recall and memo bandwidth giving It clear edge above the conventional crypto algorithm. because A result of judgment because A result of additional linked schemes, the projected method not single provide the advantage of customer solitude maintenance except in addition maintains good and sought later than properties (e.g. small Computational cost). Hence, A vehicular joint be able toward namelessly act together because A result of additional vehicular joint and nobody be able toward learn in order about the customer (e.g. location/user identification/transaction privacy).similar toward the method be base going on ECDLP, they obtain the similar security because A result of fewer bits answer similar toward evaluate toward their counterpart similar toward IFP and DLP base schemes.

References

[1] Hussain, R. ; Dept. of Comput. Sci. & Eng., Hanyang Univ., Seoul, South Korea ; Abbas, F. ; Junngab Son ; HasooEun, “Privacy-aware route tracing and revocation games in VANET-based clouds” Published in:Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference onDate of Conference:7-9 Oct. 2013Page(s):730 – 735.

[2] Hussain, R. ; Dept. of Comput. Sci. & Eng., Hanyang Univ., Seoul, South Korea ; Junggab Son ; HasooEun ; Sangjin Kim, “Rethinking Vehicular Communications: Merging VANET with cloud computing” Published in:Cloud Computing Technology and Science (CloudCom), 2012 IEEE 4th International Conference onDate of Conference:3-6 Dec. 2012 Page(s):606 – 609.

[3] Janech, J. ; Fac. of Manage. Sci. & Inf., Dept. of Software Technol., Univ. of Zilina, Zilina, Slovakia ; Lieskovsky, A. ; Krsak, E., “Comparation of Strategies for Data Replication in VANET Environment”, Published in:Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference onDate of Conference:26-29 March 2012Page(s):575 – 580

[4] Ebers, S. ; Inst. of Telematics, Univ. of Lubeck, Lubeck, Germany ; Fischer, S., “Poster: Adapter framework for VANET simulators”, Published in:Vehicular Networking Conference (VNC), 2014 IEEEDate of Conference:3-5 Dec. 2014Page(s):193 – 194.

[5] Fang Lan ; Dept. of Network Res., Inst. of Syst. Eng., Beijing, China ; Wang Chunlei ; Ma Guoqing, “A framework for network security situation awareness based on knowledge discovery”, Published in:Computer Engineering and Technology (ICCET), 2010 2nd International Conference on (Volume:1) Date of Conference:16-18 April 2010Page(s):V1-226 - V1-231.

[6] Wu Kehe ; Dept. of Comput. Sci. & Technol., North China Electr. Power Univ., Beijing,China ;Zhang Tong ; Li Wei ; Ma Gang, “Security Model Based on Network Business Security”, Published in:Computer Technology and Development, 2009. ICCTD '09. International Conference on (Volume:1)Date of Conference:13-15 Nov. 2009Page(s):577 – 580.

[7] Song-song Lu ; Sch. of Internet of Things Eng., Jiangnan Univ., Wuxi, China ; Xiao-Feng Wang ; Li Mao, “Network security situation awareness based on network simulation”, Published in:Electronics, Computer and Applications, 2014 IEEE Workshop onDate of Conference:8-9 May 2014Page(s):512 – 517.

[8] ZhihuWang ; Guangxi Econ. Manage. Cadre Coll., Nanning, China, “Design and realization of computer network security perception control system”, Published in:Communication Software and Networks (ICCSN), 2011 IEEE 3rd International Conference onDate of Conference:27-29 May 2011Page(s):163 – 166.

[9] JeongkyuHong ; Dept. of Comput. Sci., Korea Adv. Inst. of Sci. Technol., Daejeon, South Korea ; Soontae Kim, “ECC string: Flexible ECC management for low-cost

error protection of L2 caches", Published in:Computer Design (ICCD), 2012 IEEE 30th International Conference on Date of Conference:Sept. 30 2012-Oct. 3 2012Page(s):512 – 513.

[10] Tanakamaru, S. ; Dept. of Electr. Eng. & Inf. Syst., Univ. of Tokyo, Tokyo, Japan ; Esumi, A. ; Ito, M. ; Kai Li, "Post-manufacturing, 17-times acceptable raw bit error rate enhancement, dynamic codeword transition ECC scheme for highly reliable solid-state drives, SSDs", Published in:Memory Workshop (IMW), 2010 IEEE InternationalDate of Conference:16-19 May 2010Page(s):1 – 4 .

[11] XunJian ; Univ. of Illinois at Urbana-Champaign, Urbana, IL, USA ; Kumar, R., "ECC Parity: A Technique for Efficient Memory Error Resilience for Multi-Channel Memory Systems", Published in:High Performance Computing, Networking, Storage and Analysis, SC14: International Conference forDate of Conference:16-21 Nov. 2014Page(s):1035 – 1046.

[12] JangwonPark ; Sch. of Electr. Eng., Korea Univ., Seoul, South Korea ;Jongsun Park ; Bhunia, S., "VL-ECC: Variable Data-Length Error Correction Code for Embedded Memory in DSP Applications", Published in:Circuits and Systems II: Express Briefs, IEEE Transactions on (Volume:61 , Issue: 2)Page(s):120 – 124ISSN :1549-7747Date of Publication :28 November 2013Date of Current Version :20 February 2014.

[13] Dilli, O. ; Dept. of Tech. Programs, Air Force Vocational Training Sch., Izmir, Turkey ; Akcam, N. ; Koyuncu, M. ; Oguslu, E., "Secure communication tests carried out with next generation narrow band terminal in satellite and local area networks", Published in:Recent Advances in Space Technologies (RAST), 2013 6th International Conference ,Date of Conference:12-14 June 2013Page(s):493 – 498.

[14] Tien-Sheng Lin ;Electr. Eng. Nat. Taiwan Univ. Taipei, Taipei ; Tien-Sheng Lin ; Sy-Yen Kuo, "Quantum Wireless Secure Communication Protocol", Published in:Security Technology, 2007 41st Annual IEEE International Carnahan Conference, Date of Conference:8-11 Oct. 2007Page(s):146 – 155.

[15] Takizawa, M. ; Dept. of Comput. & Syst. Eng., Tokyo Denki Univ., Saitama, Japan ;Mita, H., "Secure group communication protocol for distributed systems", Published in:Computer Software and Applications Conference, 1993. COMPSAC 93. Proceedings., Seventeenth Annual InternationalDate of Conference:1-5 Nov 1993Page(s):159 – 165.

[16] Chen Zuning ; Dept. of Comput. Sci. & Technol., Xi"anJiaotong Univ., Xi"an, China ; Qin Zheng ; Wang Xianhui, "A quasi quantum secure direct communication protocol with authentication", Published in:Computer Science and Information Technology (ICCSIT), 2010 3rd IEEE International Conference on (Volume:5)Date of Conference:9-11 July 2010Page(s):48 - 52