International Journal of Engineering & Technology, 7 (4.10) (2018) 837-841

International Journal of Engineering & Technology

Website: www.sciencepubco.com/index.php/IJET

Research paper

Enhancing Security Protection using Elliptic Curve Encryption and Digital Signature in Vehicular Ad-Hoc Network

K.Selvakumar[1*], S.Naveen Kumar[2]

[1]Department of Information Technology, Annamalai University.*
[2]Department of Computer Science and Engineering, Annamalai University.
**Corresponding author E-mail: kskaucse@gmail.com*

Abstract

The Vehicular Ad-Hoc Network (VANET) is a liberality vehicle acts as remote switch or node in a cellular system. The VANET is much reasonable because of the single framework attributes agree to the system to be unbolted to metro. In this paper, we propose a Secure Hash Algorithm (SHA-1) to make an interesting key to every message. Likewise, prescribe capable and reasonable alias convention with prohibitive disconnection propagation. We set forward prime pseudonyms reasonably make a long time cycle that are worn to interact with semi-confided in experts and alternate pseudonyms with a minor lifetime which are utilized to talk with different nodes. Likewise, suggestion in the digital signature utilized in VANET is the basic, ECEDS (Elliptic Curve Encryption and Digital Signature). ECEDS enrich with system security by using a digital signature for the messages actually communicated with the system.

***Keywords**: Authentication, ECEDS (Elliptic Curve Encryption and Digital Signature), Pseudonyms, Security, VANET (Vehicular Ad-Hoc Network).*

1. Introduction

Vehicles associated with each other's throughout an ad-hoc pattern to design a wireless framework called "Vehicular Ad-Hoc Network". A VANET is sprouting innovations builds a mobile framework by through impactful vehicles as nodes. In VANET, communications are reassigned among nodes and additionally Roadside Units (RsU's). It continues as both server and customer. VANET turns each vehicle into a remote switch or vehicles, endure nodes roughly from 100 to 300 mts of one another to append and make a complex with a broad area. VANET is an advancement that incorporates the backbone of recent age remote systems to the vehicles. VANET manufacture a full-bodied ad-hoc arrangement which is surrounded by mobile nodes and roadside units as explained in Ref [1]. The movement that involves the utilization of Secure Hash Algorithm (SHA-1) makes an excellent key for every message. The ECEDS at that point cause a multi key combine signature utilizing the SHA-1 key that fuses ECEDS domain specifications. Here we send the digital signature to the goal all alongside with the message. The receivers verify the signature by utilizing SHA-1 key for the message, ECEDS and the multi key combine. In case the substantiation technique challenges single key combines, at that point the signature is checked; something else, the message was demolished on transmission. An Open Key Infrastructure (OKI) is an arrangement of jobs, access, methods to form, convey, store, and repudiate approaches and open-key encryption. The basis of an OKI is to inspire the preserved electronic swap of information for an extension of network action, for a part, web based business, web managing an account and secret mail. Three distinct arrangements of messages can be used as an open-key cryptosystems are Encrypted message, Signed message, marked and scrambled message. Testaments commonly consolidate the owner's open-key, the lapse date of the authentication, the owner's name and alternative information about the open-key owner. Operating systems (OSs) and other programs maintain preparations of confided in CDA (Certificate Distribution Authority) root authentications to confirm endorsements that a CDA has delivered and remarkable.

2. Related Work

A numeral of analyst has kept overconfident their efforts concerning privacy-preserving authentication. Here we catalogue these analyst efforts in the pseudonymous-based authentication. Many of the pseudonymous platform plans are put into operation with the assistance of Open Key Infrastructure (OKI). These methods utilize OKI dependent certificates which are emotionally involved with comparable private keys. [3] Circulate more number of pseudonyms amongst nodes which analogous private keys. In case of appreciation of a spiteful movement, the original distinctiveness is publicized by the CDA. The scheme presupposes an inescapable utilization of RsU's that add to the framework load and along these lines, the general daily practice of the framework moves forward. The CDA issue the initial pseudonym as glowing as maintain the organization between the initial pseudonym and the real identity of a node. Nonetheless, the original uniqueness in CDA's database are encrypted by other article is called as Revocation Distribution Authority (RDA) and accordingly, CDA is incapable to decrypt these original identification. Alternate pseudonyms are delivered by RsU's upon fruitful authentication of the initial pseudonym. A node then televises a communication signed with the connected private key of the alternate pseudonym and the recipient node confirms the message with a related open key arranged in the alternate pseudonym [4] – [11]. Around there, few past and improvements of SHA-1 and ECEDS are explained in [13], [14]. Nonetheless, this device estimates the prevalent distribution of RsU's. After analyzing the article, we deduct the successive limitations; pseudonymous-based arrangements incur powerful computational, communicational and capacity because of the presence of CRL (Certificate Revocation List) [12].

3. Authentication Security in VANET

3.1. Vehicular certification and initial pseudonym formation

At the time, sender/initiator node (V_i) develops an arbitrary number k (This irregular value is next encrypted in CDA's Paillier open key) and a open/private ECC key pair IK_i/AK_i. V_i sends this data alongside the VID_i to CDA.

Step 1: $V_i \rightarrow$ CDA: $k\|IK_i\|VID_i$.

The V_i deliver this data to the CDA by means of some safe channel (for instance node visits the CDA). Step1 is mandatory only once.
CDA approves the VID_i. As verifies, it encrypts VID_i with single open key developed by RDA, encrypts k with its Paillier open key IK_{CAP}, produces a termination time T_{CDA} and build the successive database (DB) access.
Example of a CDA database:

CDA $\rightarrow$ DB : $(VID_i)_{PK_{RDA}}\ \|T_{CDA}\|IK_i\|k$

CDA signs $(T_{CDA}\|IK_i\|(k)_{IK_{CAP}})$, and attach it to V_i as its first initial pseudonym.

Step 2: CDA $\rightarrow$ V_i : $(T_{CDA}\|IK_i\|(k)_{IK_{CAP}})\,AK_{CDA}$

3.2. Restore initial pseudonym

Once the T_{CDA} depart, V_i requirements to get the initial pseudonym again. In such manner, V_i arbitrary preferred a few $k^{'}$, creates a open/private ECC key pair

$IK_i^{''}\ /\ AK_i^{''}$

Encrypts this information in open key of CDA along with k and deliver it to CDA by utilizing 3G/4G technology.

Step 3: $V_i \rightarrow$ CDA: $(k\|k^{'}\|IK_i^{''})\,IK_{CDA}$

In case, the node desire the restore of an initial pseudonym to CDA by means of RsU's then delivered this message to the close-by RsU's that advances this demand to the CDA. On by demand, few unique reason bits in the message utilized that empowers the RsU's to perceive the node is asking for initial pseudonym by means of RsU's or the node is asking the RsU's for a recent alternate pseudonym.

Step 3': $V_i \rightarrow$ RsU $\rightarrow$ CDA: $(k\|k^{'}\ \|IK_i^{''})\,IK_{CDA}$

CDA certify this message with perfect k, develop a new termination time $T^{'}_{CDA}$, modernize its database with unique values of $k^{'}$, $IK^{''}_i$ and T_{CDA}. CDA rehashes stage 2, yet encrypts the recently generated initial pseudonym in $IK^{''}_i$ and delivers return to V_i. In Off the chance that, the demand has originated from RsU's then CDA dispatch this message to V_i by means of RsU's alongside the signed k. The signed number of k generates a company with the advanced value of $k^{'}$. If RsU's advertises this message, V_i analyze it with aged k, prove CDA's signature, decrypt it and transformation its initial pseudonym. Because of encryption, RsU's is helpless to disclose the advanced initial pseudonym to the V_i.

Step 4: CDA $\rightarrow$: V_i $((T_{CDA^{'}}\|IK_i^{''}\|(k^{'})\,IK_{CAP})\,AK_{CDA})\,IK_i^{''}\|(k)\,AK_{CDA}$

3.3. Alternate pseudonym formation

RSU's occasionally communicates the messages while declaring the quality. Its additionally consist of the open key of the RsU's. If a node gets this message it demands for the alternate pseudonym. The node creates other open/private ECC key pair ($IK^{'}_i$, $AK^{'}_i$). It encrypts the recently created open key and initial pseudonym, $-k$ and a nonce in RsU's open key and sends it to the RsU's.

Step 5: $V_i \rightarrow$ RsU $((T_{CDA}\|IK_i\|(k)\,IK_{CAP})\,AK_{CDA}\|IK_i^{'}\|-k\|\text{nonce})\,IK_{RSU}$.

RsU's check CDA's trademark, encrypts $-k$ with Paillier open key of CDA. RsU's holding the homomorphic addition of one and the other (k) IK_{CAP} and ($-k$) IK_{CAP}, receives (S) IK_{CAP}.
Where (S) IK_{CAP} = (k) IK_{CAP} + ($-k$) IK_{CAP}, RsU's deliver the (S) IK_{CAP} to CDA for checking purpose.

Step 6: RsU $\rightarrow$ CDA: (S) IK_{CAP}

CDA decrypts S, catch O ($k + (-k) = 0$) and circulate *verifiable* message to RDA if not deliver *not verifiable*.
Step 7: CDA $\rightarrow$ RsU's: *verifiable* / *not verifiable*.
CDA receives the encrypted value and doesn't serves any idea around that node is utilizing this value. The value of $-k$ is utilized to avoid a cruel attack.
Upon earning certification that the message began from V_i, RsU's arrange a alternate pseudonym. It constructs the termination time T_{RSU}, inserts it with recently developed $IK^{'}_i$, and sends it to V_i. The IK'i must be produced by V_i each time an alternate pseudonym is asked. In any case, a node can register again in a lake of ECC key pairs.

Step 8: RsU's $\rightarrow$ V_i : $((T_{RSU}\|IK_i^{'})\,AK_{RSU})\,IK_i^{'}$.

4. Trouble Description

VANET is a rising innovation and it is now also beneath advancement. The initial security problem in VANET is scrutinized the uprightness of messages brought back amid nodes. In this paper, execution of security calculations in designing and simulation for VANET is explained. The designing and simulation of our work may utilize in numerous VANET investigations about exercises and regulates the security convention advancement for VANET gives another security way to deal with secure the message utilizing ECEDS. The accompanying advances depicted the usefulness of our execution:
(i) The seller vehicle will make a hash value for this message utilizing the SHA-1 algorithm.
(ii) The vehicle makes a digital signature for the message utilizing ECEDS.
(iii) The recipient vehicle will count the hash value for the message and confirm the digital signature.
(iv) The digital signature is confirmed, the recipient node accepts the message began from its unique seller.

5. Performance

5.1. ECEDS Domain Specification

ECEDS design needed that the private and open keys utilized for digital signature reproduction and confirmation may develop the domain specifications. The domain specification is equivalent to a club of customers and might be open. Domain specifications are in fixed for expanded time duration. [14] [15] [16] The ECDSA domain specification is:
- x or y, the span of the basic range,
- 'u' *is* the elliptic curve specification which is utilized to describe the condition of the curve,

- '*v'* is the elliptic curve specification which is utilized to characterize the condition of the curve,
- *B* = (Bg, *Bh*), a mark on the elliptic curve, also known a base value,
- *k* is the form of the base value *B*,
- *j* is the form of the elliptic curve partitioned by the request *k*, also known the cofactor.

5.2. ECEDS Private /Open Key

ECEDS key combine comprises of private key *'p'*, and an open key '*O'*. Every key pair is related to a particular arrangement of domain specifications. The private key *p*, the open key *O*, and the domain parameters may scientifically identified with each other by means of the connection *O* = *pB*, where *pB* is the entirety of *p* duplicates of the common point *B*. This is otherwise called Elliptic Curve Scalar multiply of *B* over *p*. The addition procedure is complete by utilizing an Elliptic Curve Arithmetic. The private key *p is* being utilized for a restricted timeframe (i.e. the crypto duration). Then again, the open key *O* utilized because the digital signature is produced by utilizing the related private key is now being used on the grounds that the digital signature may check. [14] [15] [16]. ECEDS private key and open key is just utilized the formation and the certification of the ECEDS digital signature. This might not utilized for different situations for example key formation. [14] [15] [16].

5.3. ECEDS Key Generation

All together the element is to create the key pair, it might guarantee that the domain specifications are substantial. Every key pair is related to the particular arrangement of domain specifications [14] [15] [16].

Accomplish the key pair is followed as:
1. Preferred an irregular number *p* in the interval [1, *n*-1].
2. Figure *O* = *pB*.
The outcomes are *p*, O, where *p* is the private key, *O* (*Og*, *Oh*) is the open key.

5.4. ECEDS Signature Formation

An article *e* signs a message by utilizing the key combine and the domain specifications. The result from the signing process is a signature and is characterized by (*a*, *b*) [14] [15] [16]. An article may trace a message as follows:
i) Preferred an integer *l*, where 1 ≤ *l* ≤ *k*-1.
ii) Process *lO* = (*g1*, *h1*).
iii) Process *a* = *g1* (mod *k*). If *a* = 0 move to stage 1.
iv) Process *l*-1 (mod *k*).
Observe: *l*-1 (mod *k*) is figured utilizing the converse hypothesis in Appendix A.
v) Process SHA-1(*e*), finally converts the string into an integer C (*e*).
vi) Register *b* = *l*-1 (C (*e*) + *pa*) (mod *k*). If *b* = 0, move to stage 1.
The signature for the message is (*a*, *b*).

5.5. ECEDS Concept Signature Confirmation

To check the signature (*a*, *b*) on a message *e*, the recipient accomplish a duplicate of the sender's domain specification, and its open key *O* [14] [15] [16]. Thus the recipient contains:
i) Check that '*a'* and '*b'* are numbers, and in the interim [1, *k*-1].
ii) Process SHA-1(*e*), what's more change this string into a number C (*e*).
iii) Register *m* = *b*-1 (mod *k*).
Observe: *b*-1 (mod *k*) is figured utilizing the converse hypothesis in Appendix A.
iv) Process *f1* = C (*e*) *m* (mod *k*), and *f2* = *am* (mod *k*).
v) Process *Z* = (*g1*, *h1*) = *f1B* + *f2O*.
vi) On the off chance that *Z* = 0, dismiss the signature. Something else, register *q* = *x1*(mod *n*).
vii) Obtain the signature when *q* = *r*.
The mark to the message *e* finally check when *q* = *a*.

6. Working Proposed Protocol

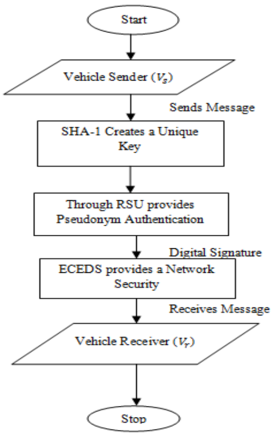
Start
Vehicle Sender (V_s)
Sends Message
SHA-1 Creates a Unique Key
Through RSU provides Pseudonym Authentication
Digital Signature
ECEDS provides a Network Security
Receives Message
Vehicle Receiver (V_r)
Stop

Fig. 1: Flow diagram for the recommended protocol

In the above Figure 1 shows the flow of the recommended protocol. The node sender V_s can transmit the message to provide the unique key with the help of SHA-1 and through RSU's it also provides the key generation based on Pseudonym authentication. After getting the key value the particular message encrypts it through the security protocol using ECEDS algorithm. Finally, the recipient node receives the proper encrypted message and decrypts the message utilizing key value which is generated by the sender node.

7. Results and Analysis

Here we assess the execution of our proposed protocol in significant viewpoints. The viewpoints to assess the execution of RSU's, where the node significantly asking the RSU's for alternate pseudonym by giving initial pseudonym. If RSU's checks the initial pseudonym essentially contains in the demand and afterward produces and deliver the alternate pseudonym to the node. Hence, it is essential to check that the RSU's is able to implement this task on a persistent condition to the nodes.

Packet Delivery Ratio (PDR)

Packet delivery ratio described as the extent of quality of information packets sent by the source node and the amount of packets gotten by the destinations node.

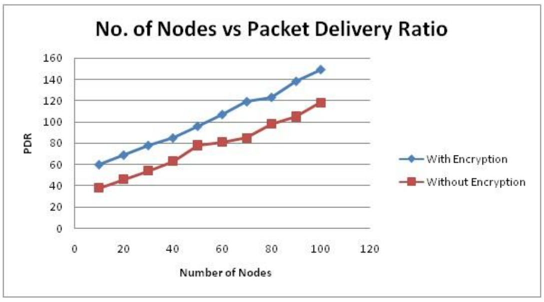

Fig. 2: Packet Delivery Ratio (PDR) with constant speed

In the above Fig.2 displays the PDR for moving nodes with constant speed. Here we have seen that 100% packet ratio for 50 nodes and finally the space constantly begins to enlarge. If the number of nodes increases to 80, the change in PDR starts increasing.

End-to-End Delay

Assign to the time taken for a packet to be broadcast across a system from source to destination.

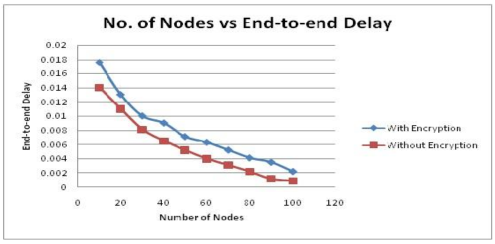

Fig. 3: End-to-end delay with time

The outcome attain from the simulation are displayed in the Figure 3 equal to the nodes moving with constant speed, and it can be observe that there is no important changes in our proposed encryptions. When the number of nodes increases to 30 the similar decrease is observed. This decrease is esteemed because of the nodes moving become more and more crowded are being collected and shows the slight decrease in delay.

Through-Put

Throughput is an amount of items passing through a system or process

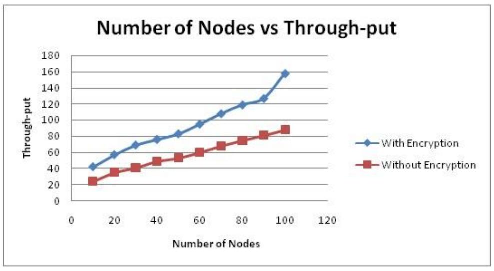

Fig. 4: Through-put w.r.t constant speed and time

In the above scenario Figure 4 it shows the throughput values for the nodes moving with constant speed. At the point the number of nodes increased to 40 the comparative increase is seen.

Packet over Head

The time it takes to exchange information on a packet-switched network. Each packet needs additional bytes of organization data that is put away in the packet header, which associates with the assembly and disassembly of packets, dismantling the general communication speed of the raw data.

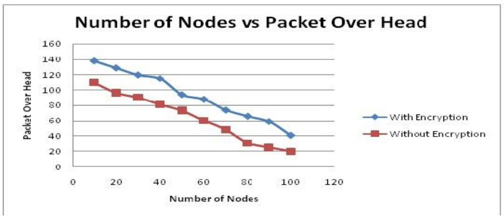

Fig. 5: Packet Over Head w.r.t speed

The outcomes seen in the simulation are observed in Figure 5 displays the outcome for the nodes with constant speed. We observed here the decreasing packet loss when the amount of nodes collects more packets because of minimization difference between them and accordingly experience more packet loss because of an impact. Be that as it may, we have seen an approximately high amount of packet drops by encryption when the quantity of nodes reaches to 50.

Data-Rate

The speed at which information is exchanged inside the computer or between a fringe gadget and the computer, estimated in bytes every second.

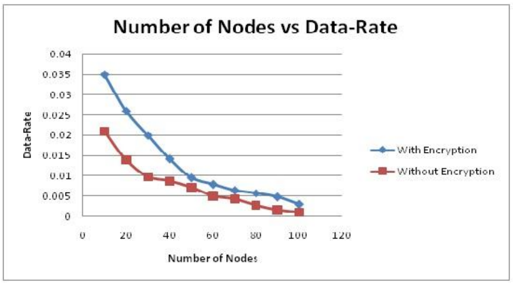

Fig. 6: Data-Rate w.r.t bytes per second

In the above Figure 6 the data-rate esteems are being noted concerning to its kilo bytes every second. The nodes are slowly diminishes and keep maintains difference between one another. We observe and slightly changes from the node 50, the sufficient value to maintain the nodes with each other constantly.

8. Conclusion

This paper proposes an efficient authentication protocol alongside upgrading security. The fundamental parts of this paper incorporate a diagram of VANETs and Pseudonym authentication. The current research challenges of VANETs broadcasting protocols are focused on issues such as ECEDS. The security examination of our proposed convention shows the flexibility across different security risk. Moreover, the act of our proposed protocol is not just to demonstrates the computational and communication overhead. We diminish the delay and maximize the security and appropriate performance.

References

[1] Pathan, Al-Sakib Khan , “Security of Self- Organizing Networks: MANET, WSN, WMN, VANET”, CRC press, 2011.

[2] Biswas, S.; Mišić, J “Proxy signature-based RSU message broadcasting in VANETs”, Communications (QBSC), 2010 25th Biennial Symposium on Communications, vol., no., May 2010, pp.5-9, 12-14.

[3] M. Raya and J. Hubaux, ‘‘The security of vehicular ad hoc networks’’, in Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw., 2005, pp. 11–21.

[4] Giorgio Calandriello, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy, ”Efficient and robust pseudonymous authentication in VANET”, In VANET ’07, New York, NY, USA, September 2007. ACM, pages 19–28.

[5] C. I. Fan, R. H. Hsu, and C. H. Tseng, “Pairing-based message authentication scheme with privacy protection in vehicular ad hoc network”, In Proceedings of the International Conference on Mobile Technology, Applications and Systems, September 2008.

[6] M. Azees, P. Vijayakumar, and L. J. Deborah, ‘‘Comprehensive survey on security services in vehicular ad-hoc networks”, IET Intell. Transp. Syst., vol. 10, no. 6, 2016, pp. 379–388.

[7] M. Raya, P. Papadimitratos, and J. Hubaux, ‘‘Securing vehicular communications’’, IEEE Wireless Commun. Lett., vol. 13, no. 1, Oct. 2006, pp. 8–15.

[8] Y. Sun, R. Lu, X. Lin, and X. Shen, ‘‘An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications’’, IEEE Trans. Veh. Technol., vol. 59, no. 7, Sep. 2010, pp. 3589–3603.

[9] L. Zhang, Q. Wu, A. Solanas, and F. J. Domingo, ‘‘A scalable robust authentication protocol for secure vehicular communications’’, IEEE Trans. Veh. Technol., vol. 59, no. 4, May 2010, pp. 1606–1617.

[10] H. Xiong, K. Beznosov, Z. Qin, and M. Ripeanu, ‘‘Efficient and spontaneous privacy-preserving protocol for secure vehicular communication’’, in Proc. IEEE Int. Conf. Commun. (ICC), May 2010, pp. 1–6.

[11] J. Petit, F. Schaub, M. Feiri, and F. Kargl, ‘‘Pseudonym schemes in vehicular networks: A survey’’, IEEE Commun. Surveys Tut., vol. 17, no. 1, 2015, 1st Quart., pp. 228–255.

[12] Studer, A.; Shi, E.; Fan Bai; Perrig, A, “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs”, Sensor,

Mesh and Ad Hoc Communications and Networks, SECON '09. 6th Annual IEEE Communications Society Conference on, vol., no., June 2009, pp.1-9, 22-26.

[13] Manvi, S.S.; Kakkasageri, M.S.; Adiga, D.G, “Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach”, Future Computer and Communication, ICFCC 2009. International Conference on , vol., no., April 2009, pp.16-20, 3-5.

[14] “Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)”, ANSI X9.62-2005, American National Standards Institute, November 2005.

[15] “Digital Signature Standard (DSS)”, FIPS 186-3, 2009. Federal Information Standards, , June 2009, National Institute of Standards and Technology, Processing Publication 186-3.

[16] SEC1 Standards for Efficient Cryptography Group, SEC 1: Elliptic Curve Cryptography, Version 2.0, 2009.