BVG Trust

J. Sci. Trans. Environ. Technov. 2017, 11(1) : 46-49

Scientific Transactions in Environment and Technovation

Enhancing Secure Service Authentication Protocol For Vanets

R.Suganya, K.Ravikumar* and R.Shanthini

Research Scholar, Karpagam University, Coimbatore.
Department of Computer Science, Tamil University, Thanjavur.
Department of Computer Science, T.U.K. Arts College, Karanthai, Thanjavur.

https://doi.org/10.56343/STET.116.011.001.008
http://stetjournals.com

Abstract

Vehicular Ad Hoc Networks **(VANETs)**, adopt the public key Infrastructure, Enhancing Secure Service Authentication Protocol for VANET's (ESSAP) security (Albert waset and Xueminshen *et al*.,2013). ESSAP originates from VANET security and it the unique aspect of ESSAP network.However, it relies on a common aspect of VANET security such as attacks, Data integrity, access control, collision avoidance and trusted authority. Fixed RSUs, which are connected to the backbone network, must be in place to facilitate communication. The number and distribution of roadside units which dependent on the communication protocol is to be used. These techniques are very effective in generating docket and adding nodes to ESSAP environment.It is observed that the proposed approach shows good performance and provide significant results in terms of time cash and reducing the number of vulnerable attacks.ESSAP can significantly eliminate bogus user due to the CDK, compared to the BAT and EMAP which mainly avoid DOS-tolerant signature scheme for VANET. This research work could be extended and tested with various advanced threats and attacks. This research work can also be implemented in SHA & TESLA.

Key words: VANETs,GPS,ESSAP,SHA,TESLA,CDK

Received : September 2015 Revised and Accepted : September 2017

INTRODUICTION

The security and privacy in VANETs face many challenges due to the open broadcasting of wireless communications and the high speed mobility of the vehicles (Yixinjiang *et al*.,2009;Halsch *et al*.,2007). It is obvious that any malicious behaviors of user, such as injecting beacons with false information, modifying and replying the disseminated messages, could be fatal to the other users. ESSAP for VANET's facilitates communication among vehicles with self organized network. This system will initialize with two nodes are Interactive Node and Non-Interactive Node. These nodes will enter in the ESSAP environment via Road Side Unit (RSU) and it acts as the gateway. Moreover ESSAP environment has Trusted Authority (TA) and Service Provider (SP) and these units are responsible for Docket Generation and collecting the information of every known Nodes. In addition ESSAP uses novel probabilistic techniques called ECC in ESSAP which provides high security to this environment.

OBJECTIVE

ESSAP for VANET provides secure and efficient service to all nodes in the environment. Since vehicles communicate through wireless channels, a variety of attacks such as injecting beacons, modifying and replacing the disseminated messages can be easily launched. A Security attacks on VANET's can have severe harmful or fatal consequences to legitimate users Gerlach *et al*.,2007. ESSAP provides enhanced security to all the available nodes by generating the authenticated Docket using secret Random key generation which implement ECC.The system model consideration consists of the following:

- **Trusted Authority (TA)**: A Trusted Authority, which is responsible for providing anonymous dockets and distributing secret keys to all OBUs in the network.
- **Road Side Units (RSU)**: RSUs, are fixed units distributed all over the network. The RSUs can communicate securely with the TA.
- **On Board Unit (OBU)**: OBUs, are embedded in vehicles. OBUs can communicate either with other OBUs through V2V communications or with RSUs through V2I communications.
- **Nodes**: Nodes will periodically exchange messages with the RSU within its region. Each vehicle is equipped with sensing and processing units.

*Corresponding Author :
email: *ravikasi2001@yahoo.com*

P - ISSN 0973 - 9157
E - ISSN 2393 - 9249

- **Tamper Proof Device (TPD)**: Each vehicle, which can be securely resynchronized, when passing by a trusted road side base station.

CONTRIBUTIONS OF THE RESEARCH

This research work contributes the following phases to the field of VANET.

Phase 1: Aggregate Network Data: It constructs the ESSAP environment with known Node, if unknown Node requested to any known node for communication, ESSAP gathers their parameters and makes it as known Node.

Phase 2: Docket Generation: Dockets are generated by ESSAP server to each node uniquely to assure authentication. This docket will initiate connection and acts as entry card for each node. To start their communication among nodes in ESSAP environment a secure CDK will be derived from their parameters using random generation algorithm.

Phase 3: ECC Encryption: The CDK will be derive using valid string 'S' which is gathered from the nodes uniquely. These strings are encrypted using ECC and makes this as EString. This EString helps to derive the CDK. This CDK will randomly change and it could not be predicted even by the ESSAP environment.

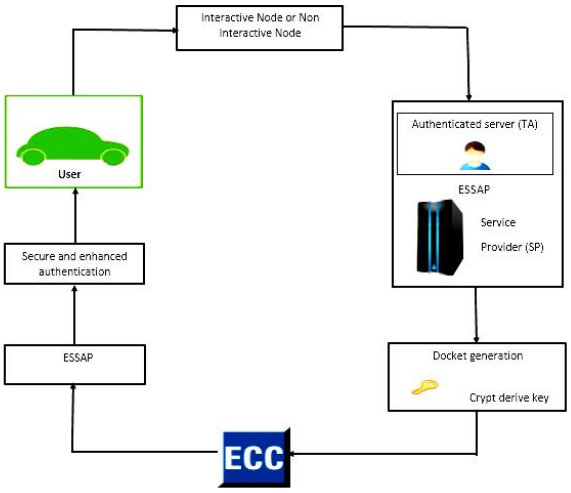

Figure 1.ESSAP Architecture

Procedure for Docket Generation

Phase 1: Identifies the N Interactive Node in V_n.

Phase 2: Collect Information on IP, System Name, Date and Time for each N.

Phase 3: Concatenate the above information of node N as IP+SystemName+Date+Time

Phase 4: Repeat the Phase 3 for all N_1……N_i and concatenate the information of N_1…….N_i to get valid string S.

Phase 5: Encrypt the valid string S using ECC Algorithm (Algorithm 3).

Phase 6: Reverse the Encrypted String E_s.

Phase 7: Generate a Random Number R_n using Random Generation Algorithm(Algorithm 4)

Phase 8: Use the Random Number R_n Multiplies at R_n times on the Encrypted String E_s and fetch each char C at every multiplies.

Phase 9 : If string length S_1 is less than the R_n times then continue the R_n multiplies at String Length at 0.

Phase 10: The char $C_{1...9}$ is combined to form a Docket and Distributed to the Interactive Node in the Network.

The network is constructed with known Node (N1 and N2).If an unknown Node N_i wants to join in ESSAP network, it has to send a Join-REQ to the Service Granter who relies on the network. Even if number nodes send a Join-REQ to Service Granter at the same time, it is easy to ensure that all requests are distinct. The signer simply pretends her public key to every request. The implicit prefix need not be transmitted with the request. The SG will authenticate each request either as Interactive Node or an Non-Interactive Node by issuing key to each request. The keys are verifiable when the nodes initialize its communication process. For security, ESSAP introduce additional constraints to that an aggregate docket. It is valid only if it is distinct from each other. This constraint is satisfied naturally for each node by Random multiplies R_n.

Then the Node N_i submits its key K to R(N).The Request Node R(N) will pass the key 'K' to the nearest or neighbor nodes are available in the ESSAP network which indicated that seeks permission to get connect with the Request Node R(N).The neighbor node verifies the Request R(N) and pass a key 'K' to both the nodes. Then the received key will be passing to the node who wants to join the networks. If the key K matches then R(N) establish connection to N,this procedure was iterated to every node who wants to join in ESSAP.

RANDOM NUMBER GENERATOR

A Random Number Generator (RNG) is a computational or physical designed to generate a sequence of numbers or symbols that lack any pattern appear random, several computational methods for random number generation exits. In ESSAP Random Number Generator have a timer value it was set as 15 and its maximum value as 30 seconds. The time will

auto start when ESSAP user enters in the systems.Many application of randomness have led to the development of several different methods for generating random data. Many of these have existed since ancient times, including deice, win flipping, the shuffling of playing cards the use of yarrow stalks in the Iching and many other techniques.

Procedure for Random Number Generator

Phase 1: Initialize the Timer Min Value as 15 and Max Value as 30

Phase 2: Auto Start the timer

Phase 3: R_n=Nk*Nb*(Nr+1)

Phase 4: Auto Stop the Timer

IMPLEMENT ELLIPTIC CURVE CRYPTOGRAPHY IN ESSAP

The two categories of nodes is primary and secondary node imitate the ESSAP network. The nodes are available in the ESSAP network once starts their communication they agree on an elliptic curve and pick a certain listening in Node(N1) who request the network communication then picks a random number which does not have to be a point on the curve. The random number (AS) was generated using random number generation algorithm and it computes. AP=AS*F.AP is defined as the point on the curve, because it is a multiple of F.In ESSAP, the proof of security for our system makes use of ECC algorithm. This security is similar to chosen ciphertext security. Roughly speaking, a public key encryption scheme is a one-way encryption. In ESSAP, the encryption process was done automatically by the system itself and the encryption algorithm is fundamentally the ECC encryption algorithm Fonseca *et al*., 2007. The first step is to collect the valid string 'S' from the node and encrypt using ECC.

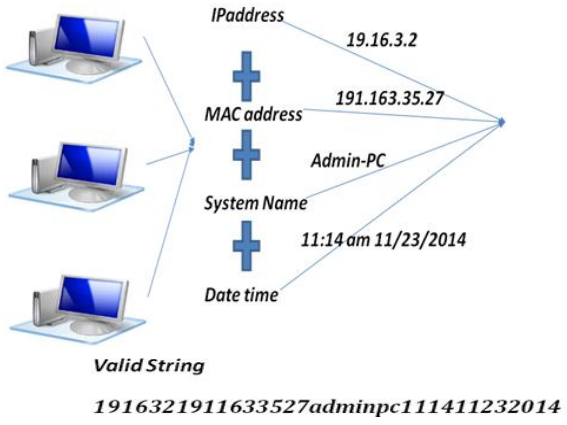

Figure 2. Encrypt Valid String

Encoding is processed byte by byte.AS encoding is ended the coded bits are processed in the reverse order from the order in which they supposed to be transmitted and RNG has a timer value.

RESULTS AND DISCUSSION

i) Performance Evaluation

To compare the ESSAP scheme with both EMAP and BAT and the basic scheme in terms of the verification complexity. Elliptic Curve Cryptography, the bit size of the public key in ESSAP is about twice the size of the security level measured. Considering the computational capacity of vehicles, the time comparison of the proposed approaches is evaluated. Time cost C_t of performance evaluation constraints are used in this validation and the docket encryption and generation scheme is evaluated.

ii) CDK Lifetime

Each encrypted message ESSAP will hold a Crypt Derive Key and it will be changed frequently for every fraction of seconds .If the intruders attempt to predict the CDK they cannot identify because it will be changed continuously (Torrent-Moreno,2007; huang *et al*.,2005). Each anonymous key should be used only with a sequence of consecutive message.Otherwise, a global attacker can extract information if a key is reused, even on different days. In ESSAP lifetime of CDK must be very short, around one day, to limit the effect of key compromises.

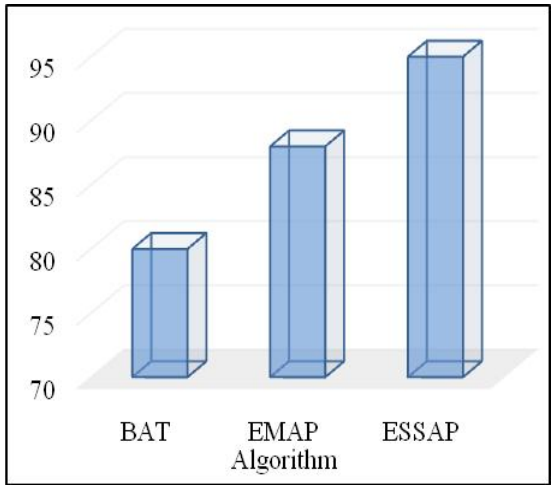

Figure 3. Performance Analysis

In proposed scheme, it tries to reduce multi-node key storage. The comparison of key storage sender and recipient among cryptographic scheme and others. It is proved that the key size of the ECC is very less when compared with the other algorithm such as, AES, DES,RSA,SHA,MD5.

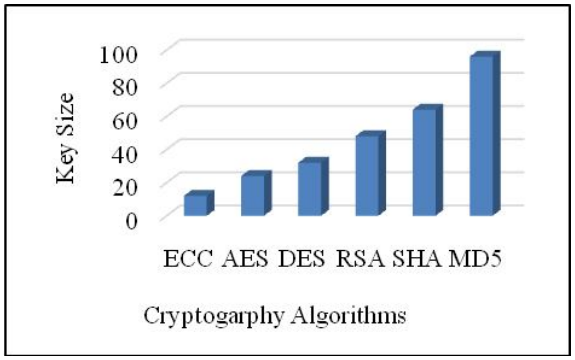

Figure 4. Key size Comparison

(iii)Traffic Analysis

In order to properly estimate the real time traffic vehicular nodes different existing techniques are considered (Jiang *et al*.,2008. Schmidt-Eisenlohr *et al*.,2007). The vehicular nodes are driving with randomly fluctuated speed. Each vehicle is randomly scattered on one intersection of the roads and repeatedly moved towards another randomly selected path. The node in ESSAP environment will provide good result.

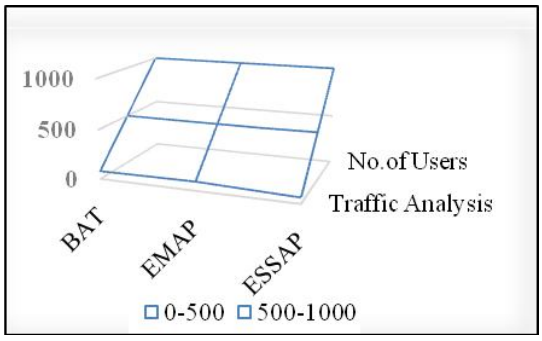

Figure 5. Traffic Analysis

CONCLUSION

VANET environment has been developed based on Docket Generation scheme Sampigethaya *et al*.,2005 . Efficient network data collection techniques are used in this research work. In order to improve the security and efficiency along with network data collection and docket generation it uses ECC encryption along with Random Number Generation. This technique is very effective in generating docket and adding nodes to ESSAP environment.It was observed that the proposed approach showed good performance and provides significant results in terms of time cash and reducing the number of vulnerable attacks.

SCOPE AND APPLICABILITY

ESSAP can significantly eliminate bogus user due to the CDK, compared with the other schemes. In ESSAP each OBU is equipped with a Hardware Security Module (HSM), which is a tamper-resistant module used to store the secure parameter of nodes, e.g., secret keys, dockets, IP, MAC, SysName, etc., of the nodes are responsible for performing all the cryptographic operations such as signing messages, verifying dockets, keys updating, EString etc. The intruders and system will not predict the key because it will be changed frequently when it requests service again checks the CDK for authenticity.

REFERENCES

Fonseca, E., Festag, A., Baldessari, R. and Aguiar, R. 2007. Support of Anonymity in VANETs – Putting Pseudonymity into Practice. In : Proc. WCNC, Hong Kong. https://doi.org/10.1109/WCNC.2007.625

Gerlach, M. ,Festag, A. and Leinmuller, T. 2007. Security Architecture for Vehicular Communication. In : Proc. WIT, Hamburg, Germany.P. 119–124.

Harsch, C., Festag, A. and Papadimitratos, P. 2007. Secure Position-Based Routing for VANETs. In : VTC Fall, Baltimore, MD, USA. https://doi.org/10.1109/VETECF.2007.22

Huang, L., Matsuura, K., Yamane, H. and Sezaki, K. 2005. Enhancing wireless location privacy using silent period. In: IEEE Wireless Communications and Networking Conference (WCNC). P.1187–1192.

Jiang, D., Chen, Q., and Delgrossi, L. 2008. Optimal data rate selection for vehicle safety communications. In Proc. 5th ACM Int.,Workshop on Veh. Inter-NETworking (VANET), San Francisco. PMCid:PMC2615073 https://doi.org/10.1145/1410043.1410050

Schmidt-Eisenlohr, F., Torrent-Moreno, M., Mittag, J. and Hartenstein, H. 2008. Simulation Platform for Inter-Vehicle Communications and Analysis of Periodic Information Exchange. In : Proc. WONS, Obergurgl, Austria. https://doi.org/10.1109/WONS.2007.340475

Torrent-Moreno, M. 2007. Inter-Vehicle Communications: Assessing Information Dissemination under Safety Constraints. In : Proc. WONS, Obergurgl, Austria. https://doi.org/10.1109/WONS.2007.340471

Yixinjiang, MinghuiShi, XueminShen. 2009. BAT :A Robust Signature Scheme for Vehicular Networks Using Binary Authentication tree. In: IEEE Transaction on Wireless Communication.