IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

A Dynamic Key Based Authentication Using Vehicular Ad-Hoc Network Communication

R. Suganya

Department of Computer Science, Tamilavel Umamaheswaranar Karanthai Arts college, Thanjavur, India

**Corresponding Author: mailtosuha@gmail.com*

Available online at: www.ijcseonline.org

Accepted: 14/Jun/2018, Published: 30/Jun/2018

***Abstract*—** A vehicular Ad-hoc network is an ad-hoc network of vehicles supported by fixed infrastructure. It is characterized by a highly dynamic topology with vehicles moving in a restricted road environment with different speeds. Vehicles are equipped with wireless communication devices known as On-Board Units (OBU) which enables them to communicate with other vehicles and Roadside Units. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) are two typical modes of vehicle communication in VANETs. Envisioned applications such as traffic accident prevention, battlefield control commands transmission and emergency coordination rescue arose a great deal of academic and industrial research on Vehicular Ad hoc Networks. In this research, developed a new security scheme called elliptic curve cryptography and ESSAP uses an algorithm to create the encrypted string. Using the encrypted string elliptic curve cryptography generated a docket, which will be transmitted from one node to another. The receiver node may desire to know that the docket has not been attacked in transit. In proposed research from our usage demonstrate that elliptic curve cryptography can ensure multicast source legitimacy and fundamentally upgrade the effectiveness of verification for multicast correspondence in VANETs, and our execution demonstrates that elliptic curve cryptography plan can be effortlessly conveyed in genuine vehicular ad-hoc network condition.

***Keywords*—** Elliptic curve cryptography, Key Generation, Security

I. INTRODUCTION

The development and commercialization of the VANETs' applications, concurrent transmission of information to various collectors turns into a pervasive method of correspondence. Anchoring multicast correspondence in VANETs presents various troubles that are not experienced when endeavouring to anchor unicast correspondence. Source confirmation is a standout amongst the most imperative prerequisites in multicast transmissions for VANET security. The customary point-to-point verification system (i.e. symmetric key) can't give anchor source validation on account of multicast application in VANETs [2]. The issue is that any recipient that has the mutual key can manufacture information and parodist the sender. There are a considerable measure of difficulties of VANETs' multicast applications.

In view of research observation, there are regular gathering traits existing in numerous VANET applications. A sort of established application is vehicle unit and co-agent driving. There are numerous company applications where vehicles are frequently sorted out as a gathering with comparative versatility designs and comparable perspective of the earth. For instance, in military troops' application, vehicles travel in the comparable speed and keep in the restricted separation [1].

The comparative situation is criminal following. At the point when squad cars track the got away lawbreakers, they facilitated with each other and take after the comparable development trail. So it is a characteristic inspiration to consider exploiting bunch quality for VANETs' source confirmation convention in multicast applications to diminish the long validation time in the Enhancing Secure Service Authentication Protocol (ESSAP)-based plan. Moreover, the asymmetric cryptography (for example. PKI and computerized signature plans) has high overhead, as far as time to encoding and unravelling calculation, and regarding data transmission utilization. The security messages forward to different vehicles, with multi-jump sending, the messages will be either ended by a (Road Side Unit) RSU or dropped while surpassing over their lifetimes [3]. The RSU can likewise screen and outline the activity circumstance of where it is found and report it to the movement control focus. With all the movement related data the activity control focus can produce a message. This overhead is a basic issue for the installed remote specialized gadget, for example, OBU. A few plans were proposed to anchor the source confirmation in multicast applications in view elliptic curve cryptography as abridged in area 2. Be that as it may, none of them can be embraced in VANETs' multicast applications on the grounds that the long validation time can't adjust the vehicle's dynamic topology. In this way, a superior and more

proficient plan for secure multicast source confirmation in VANET must be outlined.

II. RELATED WORK

Efficient Secure Aggregation in VANETS

In this research, the approach of secure message total, the long-lasting trademark of asset obliged sensor systems. Generally, rather than letting the accepted flooding approach deal with message spread in a VANET, this is appointed just to chosen vehicles who share a comparative perspective of their condition. They will depict a few calculations for accomplishing this and contrast them and each other. They will likewise present the idea of onion signature, which can be viewed as the partner of onion directing. Depending on reasonable reproductions, they have arrived at the conclusion that VANET security can be more productive when utilizing our conglomeration instruments. The outcomes affirm that protected aggregation is a promising methodology for expanding the channel proficiency and diminishing message conveyance delay in VANETs. Also, they have arrived at the fascinating conclusion that accumulation adds to better information rightness and, in some sense, a more elevated amount of security.

A Group Mobility Model for Ad Hoc Wireless Networks

In this research, reference point group mobility based secure transmission. Each gathering has a consistent focus. The inside's movement characterizes the whole gathering's movement conduct, including area, speed, course, increasing speed, and so on. Along these lines, the gathering direction is controlled by giving a way to the middle. As a rule, hubs are consistently conveyed inside the geographic extent of a gathering. To hub, each is alloted a reference point which takes after the gathering development. A hub is arbitrarily put in the area of its reference point at each progression. The reference point plot permits autonomous arbitrary movement conduct for every hub, notwithstanding the gathering motion. This research show that, when an ad hoc network is conveyed in a genuine circumstance, it isn't adequate to test it with arbitrary walk compose portability models since the movement example can associate in a by and large positive, yet now and then negative route with organize conventions.

Efficient and Secure Source Authentication for Multicast

In this research, TESLA is productive and has a low space overhead primarily on the grounds that it depends on symmetric-key cryptography. Since source validation is an innately topsy-turvy property (every one of the beneficiaries can confirm the credibility yet they can't create a bona fide information bundle), utilize a deferred revelation of keys to accomplish this property. So also, the information confirmation is postponed too. By and by, the verification delay is on the request of one roundtrip-time (RTT). TESLA model which gives an answer for the source validation issue under the suspicion that the sender and receiver are loosely time synchronized, Low computation overhead, Low communication overhead, Perfect loss robustness.

Message Broadcast in VANET Using Group Signature

In this research introduced a group signatures scheme empowers an individual from the gathering to sign the messages namelessly in the interest of the gathering. Such a marked message is openly certain with the general population key of the relating gathering. In any case, just the gathering chief can decide the personality of the endorser of the message. The obscurity of the gathering part is characteristically kept up. In this research, both are consolidated to give vehicle and message verification, security at area and character level also, non-revocation in one plan with less computational also, correspondence overheads. The joined plan maintains a strategic distance from multi-aggregate plans. Be that as it may, the execution of denial and overheads actuated by repudiation records needs to be considered. The impact of cryptographic and correspondence delay was re-enacted and comes about demonstrated that the postponement is critical however not an impediment to security provisioning. Communicate relief with bring down recurrence of message transmission may prompt better communicate of crisis alerts.

III. METHODOLOGY

Enhancing Secure Service Authentication Protocol

The progress and wide arrangement of remote correspondence advances have upset ESSAP framework demonstrate. It gives the best and ever accommodation and adaptable Internet get to and different kinds of individual correspondence. Moreover, by utilizing those specialized gadgets prepared in vehicles known as OBU, the vehicles would communication be able to with each other, and additionally with RSU situated at the basic focuses out and about. With the On Board Unit (OBU) and RSU a self-sorted out system can be framed and the RSU could be associated with the Internet Backbone.

An ESSAP gives correspondence of Roadside-to-Vehicle correspondence and Inter Vehicle correspondence (IVC), expects to enhance the driving wellbeing, movement administration and secure correspondence between the vehicles that goes under ESSAP condition. Moreover, restrictive security safeguarding must be accomplished as in client related private data are ensured.

Subsequently it is basic to build up a suit for security instrument. To the principal consider that arrangements with the security for IVC.

A group development in our protected source validation convention is adaptable and variable as indicated by various application situations. In this research, break down one application situation in vehicle troops for instance to show the usefulness and accessibility of Enhancing Secure Service Authentication Protocol. A squad is comprised of a few vehicles and a pioneer (The blue vehicle) is doled out in advance and filled in as a trusted authority to multicast orders to every squad part. Individuals in a squad have comparable spatial and transient qualities. For example, they have comparable decision for new heading, new goal, voyaging speed and stop/dynamic interims. In ECC, the squads could be dealt with as versatility gatherings. The gathering pioneers will multicast secure messages to group nodes.

The user in the ESSAP environment may participate in the existing network or participate in the new network. But the ESSAP environment will decide that it may be new or continue with the existing one. The user request to the server, by the Join - REQ and the server accepts the requests and sends the Authentication Key (Auk) to the client, and then the client. Submits the authenticated key to the server verification and the servers verifies the Authenticated key and allow to join the user to the ESSAP Environment. After the user registration process completed, ESSAP determine the user node as Interactive Node (N1) or Non-Interactive Node (N2). Once the Node confirms its participation, it receives a private key (P_k) is N1 (P_k). This node is known as Interactive Node.

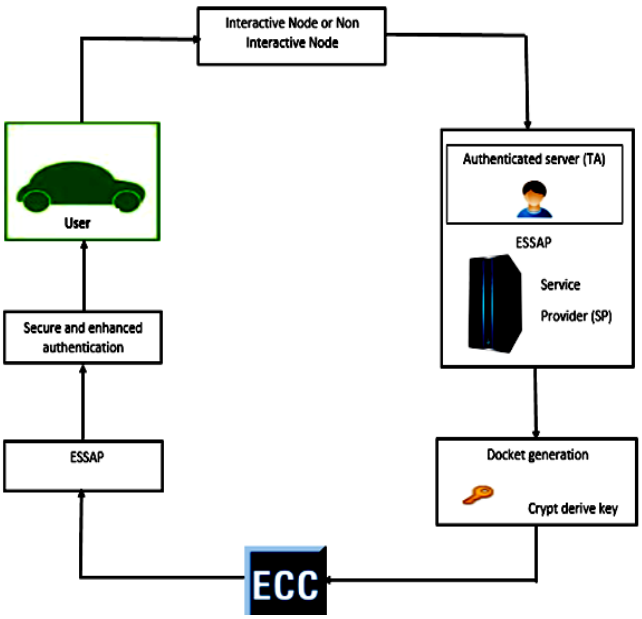

Fig 1: ESSAP Framework

The private key is issued by the Service Granter (SG) of ESSAP Architecture. This N1 (P_k) node is the initiating node of the ESSAP Environment. The nodes participated as Non-Interactive are the second participants of ESSAP network and these nodes are called as Assistant Nodes A (N). These nodes will also have the Private Key (P_k) which is received from the Service Granter (SG).The Private Key of Non-Interactive Node N2(P_k) will forwarded to the AS(Authenticate Server) it verifies that key and establish a connection to that node. This Authenticate Server is the key distribution center and it is responsible for generating and assigning related parameters for the vehicles and RSUs.

This Authenticate Server (AS) will receive the Join-REQ from both the Interactive and Non-Interactive Nodes. This is valid text string, the server sends the authentication key to the client, and thus the client submits the authenticated key to the server for verification. Unique docket will be provided to each node in the network. An elliptic curve is a set of points(x, y) for which it is true $y^2=x^3+ax+b$given certain chosen numbers a and b. Typically the numbers are integer, although in principle the system also works with real number. It uses many cryptographic algorithms. In ESSAP, ECC is used to encrypt the valid text string generated in docket generation phase and encrypted string is reversed. A Random number is implemented of random number time on the EString. At each multiples of random number a character is fetch from the Encrypted String and constructs, Docket then it is distributed to the node.

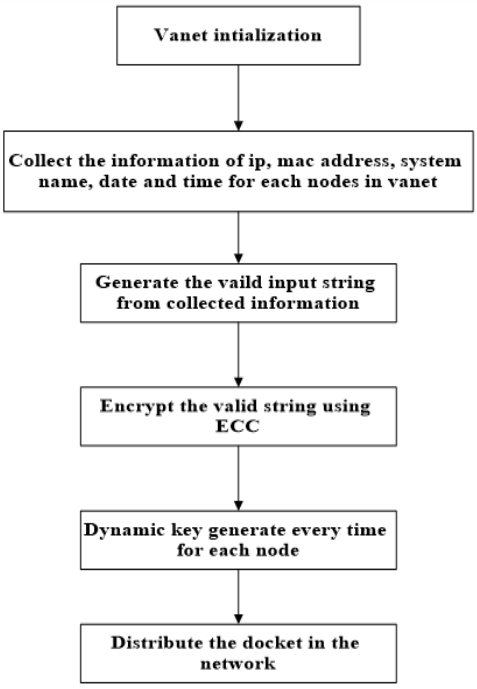

Fig 2: Key Generation

Algorithm

Identifies the N Interactive Node in V_n.
Collect Information on IP, System Name, Date and Time for each N.
Concatenate the above information of node N as
IP+SystemName+Date+Time
Repeat the Phase 3 for all N_1……N_i and concatenate the information of N_1…….N_i to get valid string S
Encrypt the valid string S using ECC Algorithm
Reverse the Encrypted String E_s.
Generate a Random Number R_n using Random Generation

```
Void rng_bytes(unsigned char*buf,int bytes)
                {
                Static unsigned int seed;
                Int I;
                If (seed==0)
                {
                Seed=(unsigned)time(NULL)
                (unsigned)clock();
                Srand(seed);
                }
                For(i=0;i<nbytes;i++)
                but[i]=rand()&OxFF;
                }
```

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.
If string length S_1 is less than the R_n times then continue the R_n multiplies at String Length at 0. The char $C_{1...9}$ is combined to form a Docket and Distributed to the Interactive Node in the Network.

IV. RESULTS AND DISCUSION

In this research, ESSAP network differ in their environment in which they are deployed. To identify several factors that affects the degree of location privacy enjoyed by the network user. Although there are several existing proposals for traditional elliptic curves. A situation could arise in further wherever the prevent curves might not be enough for secure communication and time efficiency.

Performance Analysis

In this experimental result shows that, simulation is conducted to verify efficiency of the proposed scheme in various aspects. The performance is compared with its existing techniques and proved it gives good results. In this result shows that, group signature model provide a 50% of performance analysis in this research work. A reference point group mobility provide a 60% of performance analysis in this research work. An elliptic curve cryptography provide a 30% of performance analysis in this research work. Our proposed elliptic curve cryptography provide high performance compared with other approach.

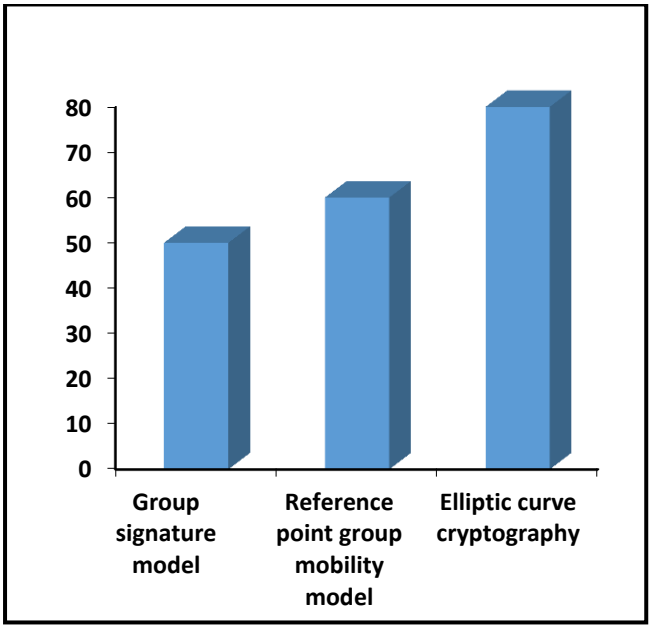

Fig 3: Performance Analysis

Time Analysis

Considering the computational capacity of vehicles, the time comparison of the proposed approaches is evaluated. The performance of the proposed approach is compared with Encryption time, Decryption time and Cryptographic operation of its existing techniques. In this result shows that, group signature model provide a 70% of time analysis in this research work. A reference point group mobility provide a 50% of time analysis in this research work. An elliptic curve cryptography provide a 30% of time analysis in this research work. Our proposed elliptic curve cryptography take less time for cryptographic operation compared with other approach.

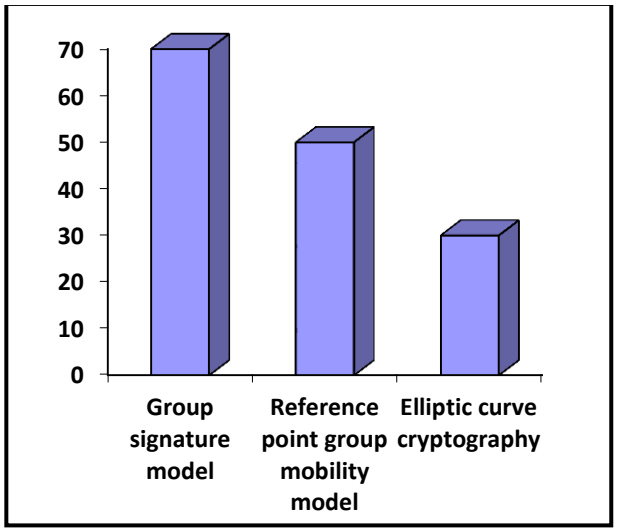

Fig 4: Time analysis

Security Analysis

A unique key is obtained from each node and their keys are unique for each. Any node receiving a key or message from another will be verified for security, that the node is working under the authorized domain. ESSAP and ECC provide higher security to the nodes of its environment. In this result shows that, group signature model provide a 40% of security analysis in this research work. A reference point group mobility provide a 60% of security analysis in this research work. An elliptic curve cryptography provide an 83% of security analysis in this research work. Our proposed elliptic curve cryptography provide high security compared with other approach.

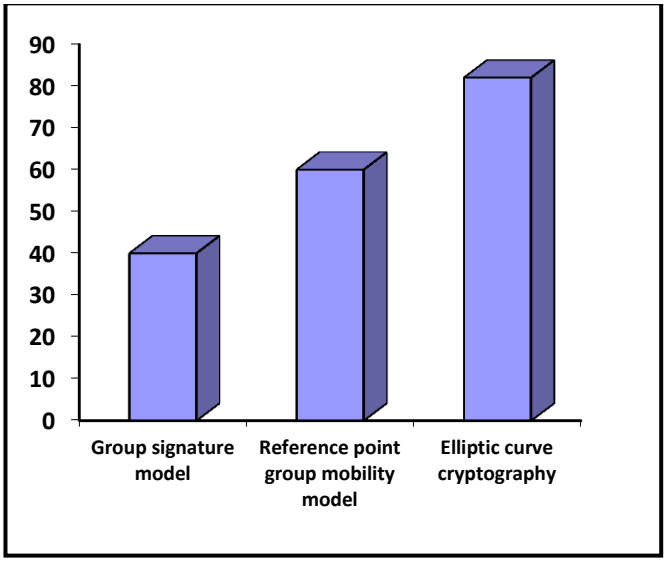

Fig 5: Security Analysis

V. CONCLUSION

In this research, proposed an Enhancing Secure Service Authentication Protocol (ESSAP) to succeed effective and secure data transmission in VANETs. ESSAP has high effectiveness in the applications where hubs have a normal gathering characteristic and offer comparative moving examples. ECC likewise exploits a mass moving example to validate data transmitted between aggregate individuals, in this manner significantly lessens the confirmation holding up time produced by ESSAP and keeps low parcel overhead and little calculation inactivity too. New approaches have been developed based on Docket Generation scheme. Efficient Aggregate Network Data techniques are used in this research work. In order to improve the security and efficiency along with Aggregate Network Data collection and docket generation it uses ECC encryption together with Random Number Generation. These techniques are very effective in generating docket and adding nodes to ESSAP environment and it is observed that the proposed approach shows good performance and provides significant results in terms of time cash and also reduce the number of vulnerable attacks.

REFERENCES

[1] X. lin, X. Sun, X. Wang, C. Zhang, P. Ho, X. Shen."TSVC: Timed Efficient and Secure Vehicular Communications with Privacy Preserving." IEEE Transactions on Wireless Communications, to appear.

[2] Studer, F.Bai, B. Bellur, and A. Perrig, "Flexible, extensible, and efficient VANET authentication", Proceeding of the 6th Annual Conference on Embedded Security in Cars (escar 2008), Noverbem 2008.

[3] A.Perrig, R.Canneti, D.Song and J.D. Tygar. "Efficient and Secure Source Authentication for Multicast" In Network and Distributed System Security Symposium, NDSS '01, Februray 2001.

[4] Chaurasia, B.K., Verma, S., Bhasker, S.M.: Message broadcast in VANETs using Group Signature. In: Fourth International Conference on Wireless Communication and Sensor Networks, pp.131-136 (2008).

[5] K.Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki. CARAVAN: providing location privacy for VANET. In Workshop on Embedded Security in Cars (ESCAR), 2005.

[6] M. Raya, A. Aziz, and J.-P. Hubaux, "Efficient secure aggregation in VANETs" in ACM Workshop on Vehicular Ad hoc Networks (VANET), 2006.

[7] H.-J. Reumerman, M. Roggero, and M. Ruffini. "The application-based clustering concept and requirements for intervehicle networks." IEEE Communications magazine, 43(4): 108-113, April 2005.

[8] H. Harney and C. Muckenhirn. Group Key Management Protocol (GKMP) architecture.RFC 2094, 1997.

[9] X.Hong, M.Gerla, G.Pei, and C.Chiang. A group mobility model for ad hoc wireless networks. In Proceedings of the ACM International Workshop on Modeling and Simulation of Wireless and Mobile Systems (MSWiM), August 1999.

