International Journal of Electrical and Computer Engineering (IJECE)
Vol.8, No.6, December 2018, pp. 5268~5277
ISSN: 2088-8708, DOI: 10.11591/ijece.v8i6.pp5268-5277

A Computational Analysis of ECC Based Novel Authentication Scheme in VANET

Sachin P. Godse, Parikshit N. Mahalle
Department of Computer Engineering, Sinhgad Institutes, Smt. Kashibai Navale College of Engineering, Savitribai Phule Pune University, India

Article Info

Article history:

Received Mar 13, 2018
Revised Jun 4, 2018
Accepted Jul 4, 2018

Keyword:

AECC
Authentication
ECC
EECC
VANET security

ABSTRACT

A recent development in the adhoc network is a vehicular network called VANET (Vehicular Adhoc Network). Intelligent Transportation System is the Intelligent application of VANET. Due to open nature of VANET attacker can launch various kind of attack. As VANET messages are deal with very crucial information's which may save the life of passengers by avoiding accidents, save the time of people on a trip, exchange of secret information etc., because of this security is must be in the VANET. To ensure the highest level of security the network should be free from attackers, there by all information pass among nodes in the network must be reliable i.e. should be originated by an authenticated node. Authentication is the first line of security in VANET; it avoids nonregistered vehicle in the network. Previous research come up with some Cryptographic, Trust based, Id based, Group signature based authentication schemes. A speed of authentication and privacy preservation is important parameters in VANET authentication. This paper addresses the computational analysis of authentication schemes based on ECC. We started analysis from comparing plain ECC with our proposed AECC (Adaptive Elliptic Curve Cryptography) and EECC (Enhanced Elliptic Curve Cryptography). The result of analysis shows proposed schemes improve speed and security of authentication. In AECC key size is adaptive i.e. different sizes of keys are generated during key generation phase. Three ranges are specified for key sizes small, large and medium. In EECC we added an extra parameter during transmission of information from the vehicle to RSU for key generation. Schemes of authentications are evaluated by comparative analysis of time required for authentication and key breaking possibilities of keys used in authentication.

Corresponding Author:

Sachin P. Godse,
Department of Computer Engineering, Sinhgad Institutes,
Smt. Kashibai Navale College of Engineering,
Savitribai Phule Pune University, Pune 411041, India.
Email: sachin.gds@gmail.com

1. INTRODUCTION

The vehicular ad hoc network (VANET) is a sub type of MANET (Mobile Adhoc Network). Moving vehicles and stationary RSU act as nodes in the network. It is rising area of research. It provides intelligent transportation management by improving safety in driving, traffic optimization, and comfort in driving to driver/owner.

Each vehicle in the network can send and receive messages by On Board Unit (OBU) and equipped with Event Data Recorder, GPS, Trusted component etc. The Roadside Units (RSU) is responsible for broadcasting safety messages periodically. Communication in VANET mainly takes place in three different ways V2V (Vehicle to Vehicle), V2I (Vehicle to infrastructure), and I2I (Infrastructure to Infrastructure).

Due to an openness of VANET, outsider nodes can enter in to the network. Security is a bigger challenge in VANET [8]. A attacker node can carry different attacks to disturb the working of network. Considering these security problems, participated node in the network must be trusted by proper authentication. Because of dynamic nature of network vehicles are very less time to establish communication with each other and to RSU.

Time required for communication also affect the effectiveness of communication in VANET. This paper first addresses a proposed scheme and its variation to improve time and security of authentication, over traditional scheme like RSA. In analysis part, we implemented plain ECC in VANET and compare with our proposed scheme implementation i.e. AECC and EECC. In this paper section 1 addressed basic of VANET. Section 2 gives related work done in the Authentication of VANET. Section 3 gives proposed novel schemes. Section 4 gives computational analysis on the basis of result recorded in Vsim (VANET Simulator). Section 5 concludes the paper.

VANET scenario is as shown in Figure 1. It gives different types of communication. As shown in the figure vehicle can communicate with other vehicle via V2V communication, vehicle can communicate with infrastructure (RSU) through V2I communication, vehicle can communicate with road side infrastructure using V2R communication [1]. Vehicle to sensor communication is depicted by V2S.

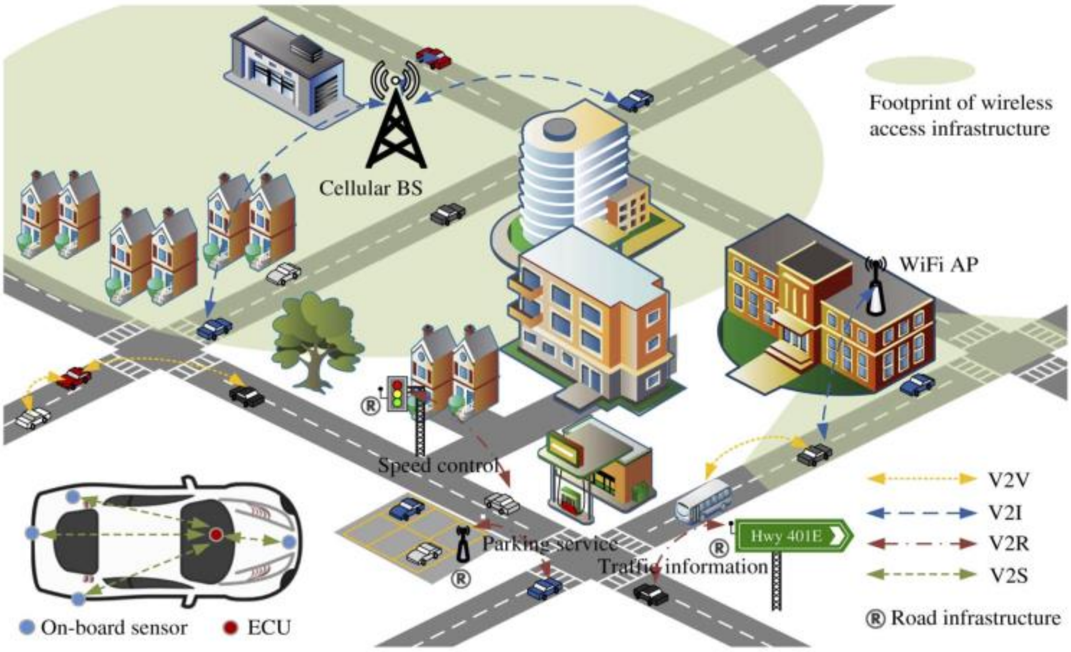


Figure 1. System architecture in VANET's

2. RELATED WORKS ON AUTHENTICATION IN VANET

Table 1 show the detailed survey of research in VANET their strength, weakness and future scope of research. Literature survey shows that over all time required for digital signature generation and verification of message in V2V communication requires more time in some schemes, which degrades performance of network. In some schemes security can hamper, If CA, RA or RSU compromise. Space required storing private keys and certificates also are an issue in some scheme. Time required for waiting, packet accessing and decision taking is also affect on performance. We found that, there is need of more research in authentication of VANET to improve authentication speed and security in VANET.

Table 1. Comparative Analysis of Existing Authentication Scheme in VANET

Reference	Scheme	Strength	Weakness	Future Scope
[9] 2016	A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET	1. No need of storage for storing a large pool of pseudonyms. 2. Certificate Revocation List (CRL) is not required. 3. Information is secured as compared to server.	1. CA, RA or RSU can compromise which can result in scheme failure.	1. Authentication process speed can improve. 2. Trust value of CA, RA and RSU can be used to find compromise node.
[10] 2016	Security Enhancement in Group Based Authentication for VANET	1. Prposed framework is secure and preserves privacy. 2. No need to sign message in V2V communication which leads to faster authentication.	1. Signature generation and verification of message requires more time which degrades performance of network.	1. Improvement in Digitial signature process. 2. Can improve process of authentication.
[11] 2016	Vehicular Authentication Security Scheme (VASS)	1. Required less computation effort as compared to other methods in hash function 2. Security is provided with privacy, authentication and Sybil attack detection.	1. It not consider vehicle to infrastructure communication	1. Vehicle to Infrastructure authentication can be possible.
[12] 2016	Secure and distributed certification system architecture for safety message authentication in VANET	1. False public-key certification is avoided. 2. Distributed certification system with high security. 3. Each RCA delegates subordinates RSUs for the Certificate management and hence increasing its availability for the vehicles.	1. Large storage required to Each vehicle for keys and certificate. 2. High transmission range required to transmit various safety messages.	1. by reducing the key sizes speed of authentication can increase.
[13] 2016	A Secure and Efficient V2V Authentication Method in Heavy Traffic Environment	1. Accelerates message processing by sending a low data volume for Communication in areas of heavy traffic. 2.Blocks replay attacks by checking time stamps	1. Vehicle to infrastructure communication not considered.	1. Vehicle to Infrastructure authentication can be provided.
[3] 2014	An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks	1. Advanced secure scheme based on Clustering and Key Distribution (SCKD) among members and cluster-heads in VANET. 2. Secure end to end communication scheme.	1. Required more memory to store keys, certificates etc. 2. Large traffic overhead 3. If CA fail all network will fail.	1. On road storage terminals are installed to store every vehicle secure data. 2. CA replica which work when primary CA fails.
[14] 2014	Threshold Cryptography-based Group Authentication (TCGA)	1. Alleviates the effect of battery exhaustion attack 2. Take less computational time as compare to GA. 3. TCGA scheme is light weight and scalable, best suited for IoT .	1. Nodes are stationary need to adapt as per VANET scenario.	1. Can be adapting for dynamic network scenario.
[15] 2016	Distributed Access Control and Authorization model for IoT	1. The local device access time and remote device access time requires nearly same amount of time.	1. Hop by hop communication is not considered.	1. Can be modifying for vehicle and RSU Authentication.
[16] 2013	Identity Authentication and Capability based Access (IACAC) Control for the Internet of Things	1. It presents an integrated approach of authentication and access control for IoT devices. 2. It defend attacks like DoS, man-in-the-middle and replay attacks efficiently and effectively.	1. Complete Interoperability need to improve. 2. Scheme considered only IOT scenario for authentication.	1. Need to adapt as per the VANET Requirement.
[4] 2009	Secure V2V Communication With Certificate Revocations	1. Addresses the problem of access to revocation information using a concept called freshness. 2. Reduces the storage requirement at the OBU and provides a constant time algorithm.	1. If the certificate of the CA is compromised then freshness checks shall not work 2. The CoS decreases as the rate of revocation increase.	1. Private and Public key is generated by individual node and just get verified by trusted server. 2. Dynamic freshness check threshold
[5] 2013	A Categorized Trust-Based Message Reporting Scheme for VANETs	1. A categorized decentralized trust management and evaluation scheme for nodes 2. Role-based trust and experience-based trust is integrated, 3. Determine the degree of trustworthiness of a node's.	1. It only considers current message details not history 2. Piggybacking not authenticated	1. Piggyback, messages and nodes history can be used for penalty or trust building 2. Dedicated task to RSU.
[6] 2014	A social network approach to trust management in VANETs	1. Novel voting scheme, each vehicle has different voting weight according to its distance from the event. 2. The vehicle which is closer to the event possesses higher weight.	1. Time is issue in waiting for packet accessing or decision taking. 2. Piggybacking delay or forgery source	1. Authenticate source of piggybacking 2. Algorithm to select time delay for packet accessing or decision taking.

3. PROPOSED WORK

Observation made from previous research about ECC based authentication.

3.1. ECC Disadvantages:

a. ECC increases the size of the encrypted message significantly more than RSA encryption.
b. Most ECDSA implementations require a secure random generator - if the same random value is reused (for different plaintext) then the private key parameter can simply be calculated;
c. ECC is much more efficient than RSA for signature generation and decryption, but it's still much slower than symmetric algorithms;
d. Type of curve and curve parameter agreement is required in ECC algorith

From previous research survey, we found that, there is need of more research

a. To provide faster authentication in VANET with preserving security requirements.

3.2. Proposed Framework:

Figure 2 shows the framework for proposed work. It shows three different authentication schemes for VANET first one is plain ECC/ Basic ECC algorithm. The second block shows Adaptive ECC algorithm, and the third block shows Enhanced ECC algorithm. Table 2 gives terms used for AECC and EECC algorithm.

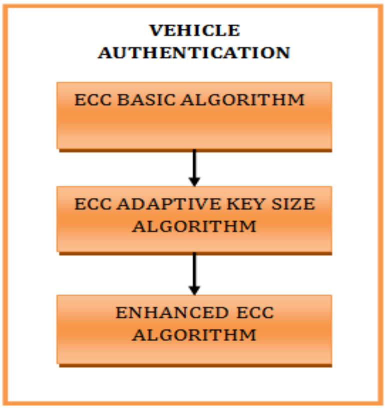


Figure 2. Framework for proposed authentication work

Table 2. Terms Used for Algorithm

Terms/Notations	Meaning
P	Key pool
Ts	Time slot.(Re-generate keys after every Ts seconds)
G	Key Generator
m,a,b	Unique parameters
K	Keys
Pu	Public key
Pr	Private key
Vc	Current vehicles
NR	neighbor RSU
Ks	Key size
Kx	new Key
Us	Public key server
Re	Verify – Sybil attack, replica attack

3.3. ECC Based Authentication: Authentication Using Elliptic Curve Cryptography

3.3.1. Elliptic Curve Cryptographic Algorithm (ECC)

ECC is an alternative mechanism for implementing public-key cryptography. Figure 3 shows elliptic curve which is considered for ECC algorithm.

The equation of an elliptic curve is given as,

y2=x3 +ax +b[7]

Terms that will be used in Cryptography using ECC,
E->Elliptic Curve
P->Point on the curve
n->Maximum limit (This should be a prime number)

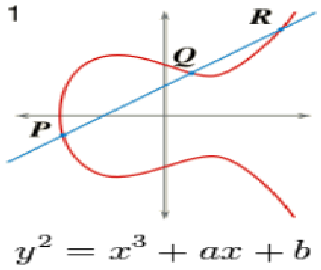


Figure 3. Elliptic curve

3.3.2. Key Generation

It is frst stage where public and private key is generated. The message is encrypted by receiver public key and the receiver is decrypting message by its own private key. Random number‘d’ selected within the range of ‘n’. Using the following equation Public key will be generate
Q=d * P
Where:
d=the random number that has been selected within the range of (1 to n-1).
P=the point on the curve.
‘Q’ is the public key and‘d’ is the private key.

3.3.3. Encryption

Let ‘m’ be the message which want to send. Ths message is represented on the curve. This has in-depth implementation details.
Consider ‘m’ has the point ‘M’ on the curve ‘E’.
Randomly select ‘k’ from [1 – (n-1)].
Two cipher texts will be generated let it be C1 and C2.
C1=k*P
C2=M + k*Q
C1 and C2 will be send.

3.3.4. Decryption:

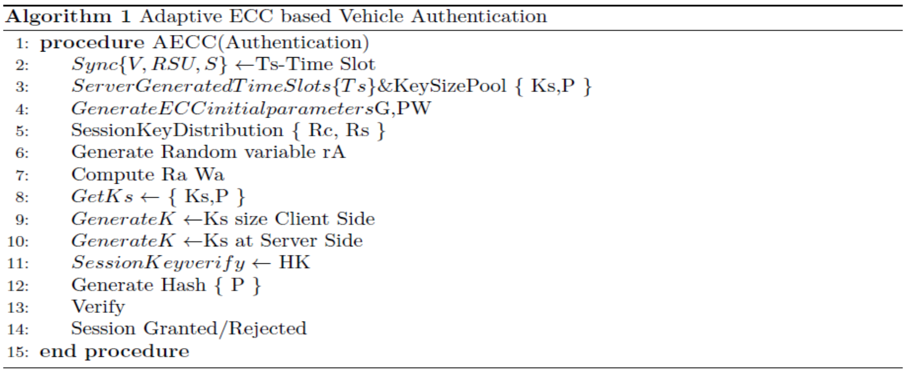
We have to get back the message ‘m’ that was send to us,
M=C2–d*C1
M is the original message that we have send.

3.4. AECC (Adaptive Elliptic Curve Cryptography) Based Authentication

AECC is variation in ECC. In this using an adaptive key size algorithm varying keys are generated. This algorithm uses the random key size where no attacker can guess, the key size at the current time, and fails to break it. In this key sizes are vary after every defined timeslot. When an attacker tries to guess the key to break the system, as the ECC is strong enough this does not happen easily. But when an attacker succeeds to do so, because of the adaptive key size (AKS) algorithm, the key is no longer relevant to that attacker.

Algorithm/Pseudo code for AECC based authentication [2]:

```
Input:
G, {Ts}, {Ks, P}, {V}
Output:
Random_Keys, Access Granted/Rejected
```

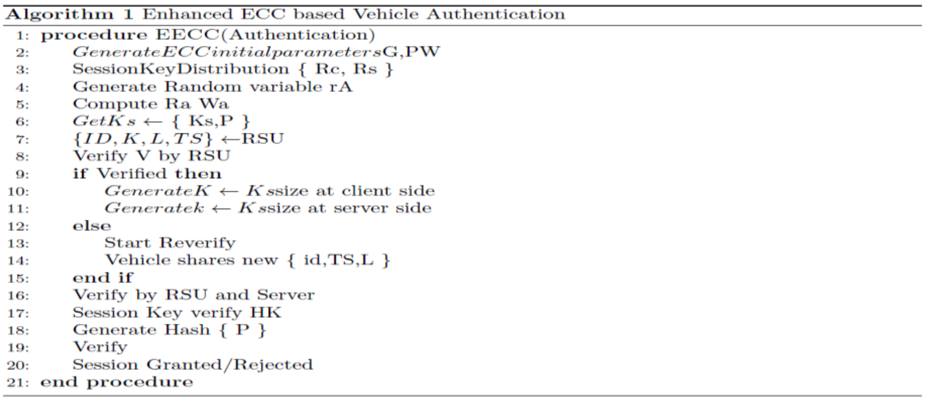


```
Algorithm 1 Adaptive ECC based Vehicle Authentication
procedure AECC(Authentication)
    $Sync\{V, RSU, S\}$ ←Ts-Time Slot
    $ServerGeneratedTimeSlots\{Ts\}$&KeySizePool { Ks,P }
    $GenerateECCinitialparameters$G,PW
    SessionKeyDistribution { Rc, Rs }
    Generate Random variable rA
    Compute Ra Wa
    $GetKs \leftarrow$ { Ks,P }
    $GenerateK$ ←Ks size Client Side
    $GenerateK$ ←Ks at Server Side
    $SessionKeyverify \leftarrow$ HK
    Generate Hash { P }
    Verify
    Session Granted/Rejected
end procedure
```

3.5. EECC (Enhanced Elliptic Curve Cryptography) Based Authentication

Enhanced ECC algorithm is extended version of AECC. In this an extra parameter is added during the transmission of information from the vehicle to the RSU for key generation. These additional parameters give the information about the vehicle ID, and the location of the vehicle from the RSU, and the other vehicle. This algorithm provides replica and Sybil attack detection along with authentication.

Algorithm/Pseudo code for EECC Based Authentication [2]:
Input:
G, {V}, {Ts}, {Ks, P}
Output:
Detect Attack, Access Granted/Rejected



```
Algorithm 1 Enhanced ECC based Vehicle Authentication
procedure EECC(Authentication)
    $GenerateECCinitialparameters$G,PW
    SessionKeyDistribution { Rc, Rs }
    Generate Random variable rA
    Compute Ra Wa
    $GetKs \leftarrow$ { Ks,P }
    $\{ID, K, L, TS\}$ ←RSU
    Verify V by RSU
    if Verified then
        $GenerateK \leftarrow Ks$size at client side
        $Generatek \leftarrow Ks$size at server side
    else
        Start Reverify
        Vehicle shares new { id,TS,L }
    end if
    Verify by RSU and Server
    Session Key verify HK
    Generate Hash { P }
    Verify
    Session Granted/Rejected
end procedure
```

4. COMPUTATIONAL ANALYSIS OF ECC & AECC

The analysis is carried out by implementing ECC and AECC in Vsim (VANET Simulator). Vsim is java based simulator for Testing, Analyzing, and implementing different protocols in VANET. We can add, create, modify scenario in simulator. Vsim provide different packages for creating VANET environment. We can load map of different cities. We can load different scenarios for same map. Figure 4 shows map of NewYork_noTS.xml is load on the VANET Simulator. Similarly we can load a map of Berlin_noTS.xml or Puebla_noTS.xml on the simulator. Or generate new map as per requirement.

Figure 5 shows uploading of New York road scenario with 2500 slow and 2500 fast vehicles with 100m communication range. Road side units are within 500m radius communication range. Vehicles are shown by small black dots and gray color circle is used for RSU. Figure 6 shows vehicle communication distance. Vehicles are shown by blue dots and blue circle show the communication range of vehicle. Each vehicle equipped with on- board unit, and every vehicle has Wi-Fi or internet. Vehicles have communication range of 100m. So vehicle can communicate with each other and with RSU. Figure 7 shows information about vehicles on the marked path. Information contains the Name, length, Max speed, Lane/direction, start location, destination location, current speed, Travel time, Travel distance, known vehicles, known messages, failed forward messages, known penalties etc.

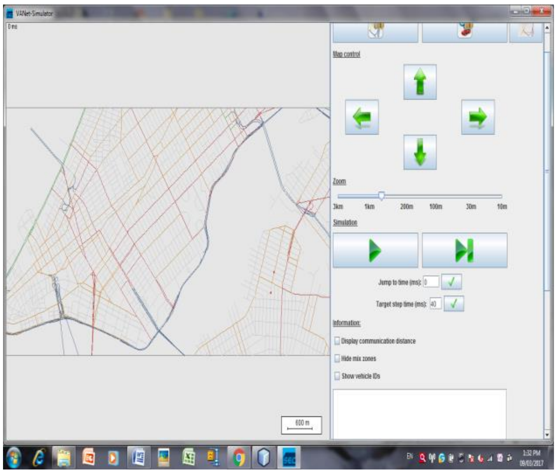
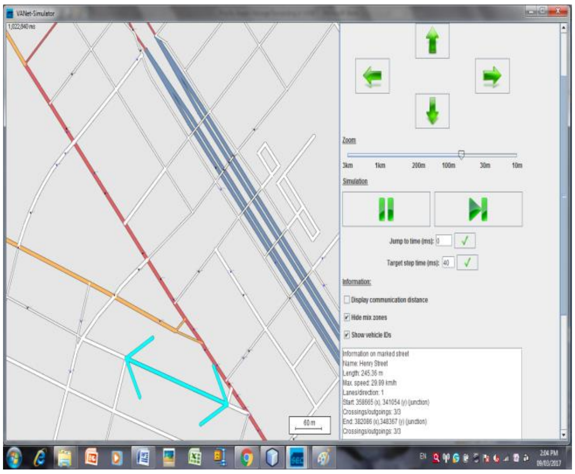


Figure 4. Map loading on VANET simulator



Information on marked street
Name: Henry Street
Length: 245.36 m
Max. speed: 29.99 km/h
Lanes/direction: 1
Start: 358665 (x), 341054 (y) (junction)
Crossings/outgoings: 3/3
End: 382086 (x),348367 (y) (junction)
Crossings/outgoings: 3/3

Figure 5. Scenario uploading in map

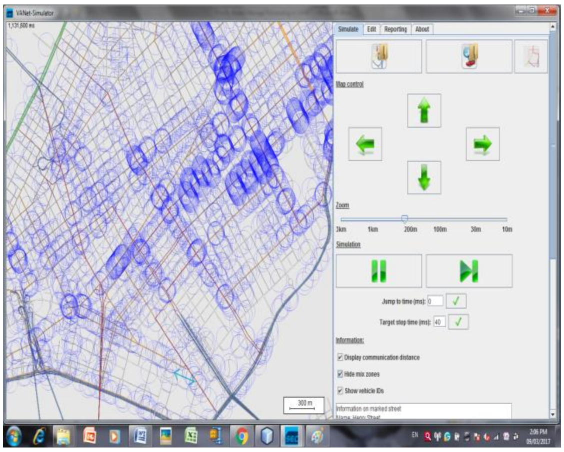
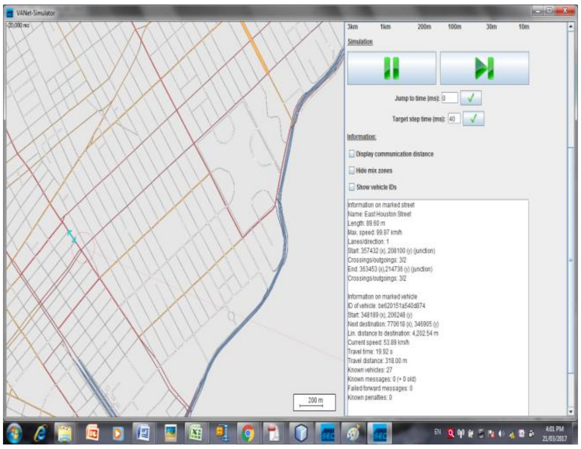


Figure 6. Vehicle communication range



Information on marked street
Name: East Houston Street
Length: 89.60 m
Max. speed: 99.97 km/h
Lanes/direction: 1
Start: 357432 (x), 208100 (y) (junction)
Crossings/outgoings: 3/2
End: 363453 (x),214736 (y) (junction)
Crossings/outgoings: 3/2

Information on marked vehicle
ID of vehicle: be620151a540d874
Start: 348189 (x), 206248 (y)
Next destination: 770618 (x), 346905 (y)
Lin. distance to destination: 4,202.54 m
Current speed: 53.89 km/h
Travel time: 19.92 s
Travel distance: 318.00 m
Known vehicles: 27
Known messages: 0 (+ 0 old)
Failed forward messages: 0
Known penalties: 0

Figure 7. Vehicle's information on marked street

Figure 8 shows graphically analysis of time required for ECC and AECC for authentication with respective iteration. In case of ECC same key is used for each iteration, and for adaptive key selected from small, large or medium group of key sizes. Graph shows that as compare to ECC, AECC required less time. So AECC is faster than ECC. Figure 9 shows that number of vehicle authenticated by AECC per second are more than ECC. Table 3 shows ECC and AECC time required for authentication. Table 4 shows number of vehicle authenticated using ECC and AECC.

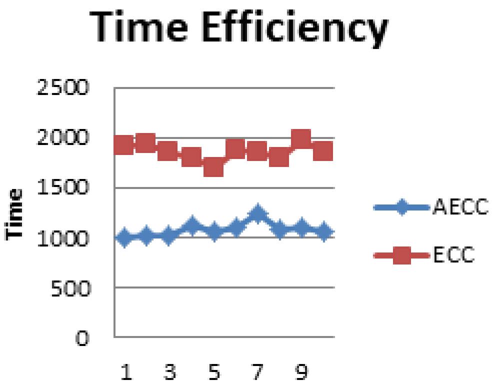


Figure 8. Time required for Authentication

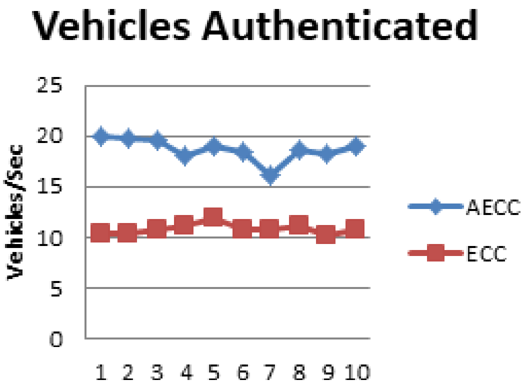


Figure 9. Number of vehicles authenticated per second

Table 3. ECC and AECC Time Required for Authentication

Iteration	ECC Algorithm	Time	Iteration	AECC Algorithm	Time
1	ECC	1924	1	AECC	1007
2	ECC	1925	2	AECC	1009
3	ECC	1854	3	AECC	1020
4	ECC	1800	4	AECC	1110
5	ECC	1688	5	AECC	1054
6	ECC	1869	6	AECC	1089
7	ECC	1846	7	AECC	1245
8	ECC	1789	8	AECC	1072
9	ECC	1966	9	AECC	1100
10	ECC	1854	10	AECC	1054

Table 4. Number of Vehicle Authenticated Using ECC and AECC

	ECC			AECC	
Iteration	Algorithm	Vehicle Authenticated	Iteration	Algorithm	Vehicle Authenticated
1	ECC	10.3950104	1	AECC	19.86097319
2	ECC	10.38961039	2	AECC	19.82160555
3	ECC	10.78748652	3	AECC	19.60784314
4	ECC	11.11111111	4	AECC	18.01801802
5	ECC	11.84834123	5	AECC	18.97533207
6	ECC	10.70090958	6	AECC	18.36547291
7	ECC	10.83423619	7	AECC	16.06425703
8	ECC	11.17942985	8	AECC	18.65671642
9	ECC	10.17293998	9	AECC	18.18181818
10	ECC	10.78748652	10	AECC	18.97533207

Security of authentication is checked by its private key breaking possibilities. Table 5 shows key breaking possibilities. Figure 10 shows that key breaking possibility of AECC is less as it takes more turn for breaking key than ECC. So AECC is more secure than ECC.

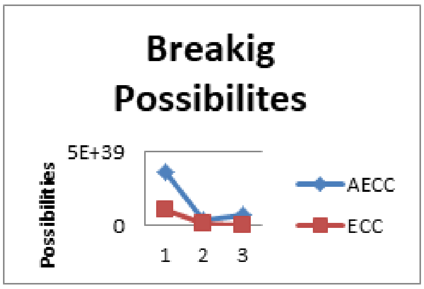


Figure 10. Key breaking possibilities

Table 5. Key breaking possibilities

Iteration	Algorithm	Breaking Possibilities	Keysize
1	ECC	1.07374E+39	256
2	ECC	1.34218E+38	512
3	ECC	1.67772E+37	1024
1	AECC	3.62388E+39	120
2	AECC	4.52985E+38	256
3	AECC	7.00227E+38	512

From above analysis we can list out following advantages of AECC

Adaptive key size algorithm it's advantages:

a. Here we using secure key selector - if the same random value is reused (for different plaintext) then the private key parameter cannot be calculated because of different key size.
b. By using less key sizes we can faster the authentication speed.
c. Here along with curve agreement, this algorithm also required key agreements.

5. CONCLUSION

Security is an important issue in VANET. Authentications prohibit entry of the unauthorized malicious user. It helps to avoid various security attacks. This paper addresses issues in authentication for improving the speed of authentication. It also takes care to maintain same or rather more security, as compared to previous authentication schemes like RSA and ECC. Here we given the computational analysis of result obtain in VANET Simulator. The time required for authentication is verified by taking multiple iteration reading, which proves that AECC required less time as compared to ECC. A number of vehicles authenticated by RSU per second are more in case of AECC than ECC; at the end security of the scheme is checked by key breaking possibility. Our needs for faster authentication reflect in improving the performance of RSU by serving more number of vehicles. In future work, we are going to add more security parameter in EECC (Enhance Elliptic Curve Cryptography) scheme. We gave an algorithm for same in this paper but an implementation is in process. Its implementation and computational analysis will be the part of our future scope.

REFERENCES

[1] Sachin Godse and Parikshit Mahalle, “Rising Issues in VANET Communication and Security: A State of Art Survey”, *International Journal of Advanced Computer Science and Applications (IJACSA)* , Vol. 8, No. 9, 2017, PP 245-252.

[2] Sachin Godse and Parikshit Mahalle, “Time-Efficient and Attack Resistant Authentication Schemes in VANET”, *Proceedings of 2nd International Conference, ICICC,* PP 579-589 2017.

[3] Ameneh Daeinabi, Akbar Ghaffarpour Rahbar, “An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks”. In*: ELSEVIER Computers and Electrical Engineering* 40 PP 517–529, 2014.

[4] Ashwin Rao, Ashish Sangwan et. al., “Secure V2V Communication with Certificate Revocations”. In: *IEEE* (2007).

[5] Merrihan Monir, Ayman Abdel-Hamid, Mohammed Abd El Aziz, “A Categorized Trust-Based Message Reporting Scheme for VANETs”. In: *Springer CCIS 381*, PP. 65–83, 2013.

[6] Zhen Huang, Sushmita Ruj et al. “A social network approach to trust management in VANETs”. In: *Springer Peer-to-Peer Netw. Appl.* (2014) 7 PP. 229–242 .

[7] Kristin Lauter, “The Advantages of elliptic Curve Cryptography For Wireless Security”. In: *IEEE Wireless Communications* 2004.

[8] Shidrokh Goudarzi, Abdul Hanan Abdullah, “A Systematic Review of Security in Vehicular Ad Hoc Network”. In: *the 2nd Symposium on Wireless Sensors and Cellular Networks (WSCN'13)* 2013.

[9] Ubaidullah Rajput, Fizza Abbas, Heekuck Oh, “A Hierarchical Privacy Preserving Pseudonymous Authentication Protocol for VANET”. In*: IEEE Access*, October 25, 2016.

[10] Rajkumar Waghmode, Rupali Gonsalves, Dayanand Ambawade, “Security Enhancement in Group Based Authentication for VANET”. In: *IEEE International Conference on Recent Trends in Electronics Information Communication Technology*, May 20-21, 2016, India.

[11] Yongchan Kim, Jongkun Lee, “A secure analysis of vehicular authentication security scheme of RSUs in VANET”. In: *Springer-Verlag France* 2016.

[12] Tiziri Oulhaci, Mawloud Omar, Fatiha Harzine, Ines Harfi,: “Secure and distributed certification system architecture for safety message authentication in VANET”. In: *Springer Science+Business Media New York* 2016

[13] Myoung-Seok Han, Sang Jun Lee,Woo-Sik Bae, “A Secure and Efficient V2V Authentication Method in Heavy Traffic Environment”. In: *Springer Science+Business Media New York* 2016.

[14] Parikshit N. Mahalle, Neeli R. Prasad and Ramjee Prasad, “Novel Threshold Cryptography-based Group Authentication (TCGA) Scheme for the Internet of Things (IoT)”, In: *proceedings of IEEE 3rd International Conference on Wireless Communications, Vehicular Technology, Information Theory and Aerospace & Electronic Systems Technology (Wireless ViTAE 2014)*. Aalborg- Denmark, May 11-14 2014.

[15] Parikshit N. Mahalle, Sandesh Mahamure, Poonam N. Railkar, Pankaj r. Chandre, “Distributed Access Control and Authorization (DACA) for Internet of Things”, In: *International Journal on Emerging Trends in Technology (IJETT)* (ISSN (Print): 2350-0808), Volume 3, Issue 3, September 2016.

[16] Parikshit N. Mahalle, Bayu Anggorojati, Neeli R. Prasad and Ramjee Prasad, “Identity Authentication and Capability based Access (IACAC) Control for the Internet of Things”, In: *Journal of Cyber Security and Mobility*, River Publishers, Volume: 1, Issue: 4, pp: 309-348, March 2013.

BIOGRAPHIES OF AUTHORS

Mr. S. P. Godse has obtained his B. E degree in Coputer Engineering from AVCOE, Savitribai Phule Pune University, Pune, India and M.E. degree in Computer Science and Engineering from Savitribai Phule Pune University, Pune, India. His areas of interest are Vehicular Adhoc Network, Mobile Adhoc Network, Natural language Processing, and Object Oriented Programming, Object Oriented Modeling, Software Engineering. He has authored 3 books on subject like: Principle of Programming Languages, Software Modeling and Design, Embedded system and Internet of Thing. Currently he is pursuing his Ph. D in Computer Engineering from Smt. Kashibai Navale College of Engineering, SPPU, Pune, India.

Dr. Parikshit N. Mahalle has obtained his B.E degree in Computer Science and Engineering from Sant Gadge Baba Amravati University, Amravati, India and M.E. degree in Computer Engineering from Savitribai Phule Pune University, Pune, India. He completed his Ph. D in Computer Science and Engineering specialization in Wireless Communication from Aalborg University, Aalborg, Denmark. He has published 56 research publications at national and international journals and conferences. He has authored 8 books on subjects like: Identity Management for Internet of Things, Identity Management Framework for Internet of Things, Data Structures and Algorithms, Theory of Computations, Fundamentals of Programming Languages, Fundamentals of Programming Languages – II, Design and Analysis of Algorithms: A Problem Solving Approach, Currently he is working as Professor and Head in Department of Computer Engineering at STES’s Smt. Kashibai Navale College of Engineering, Pune, India.