RSA Based Location Verification in Vehicular Clouds: Agent Based Approach

Shailaja S.Mudengudi, Assistant Professor, Electronics and Communication Department, Tontadarya College of Engineering, Gadag, Karnataka ,India, psmssm@gmail.com

Dr. Mahabaleshwar S.K, Associate Professor, Department of Electronics and Communication Engineering, Basaveshwar Engineering College(Autonomous), Bagalkot, Karnataka, India. mahabalesh_sk@yahoo.co.in

Abstract: **Vehicular Cloud Computing (VCC) emerged as a solution for enhanced usage of underutilized resources in the Vehicular Network. Most of the applications of VCC are location based ranging from collision avoidance to infotainment. The location information is critical which plays a vital role in making or breaking of the applications. The damage caused by the attacks on location information may range from exploiting and enjoying services more than the vehicle node has subscribed to life endangering events. In order to strengthen the location verification process, we have presented an agent based location verification method. Our method uses the hidden verifier nodes whose presence is known only to the highest trusted entity Central Authority (CA). RSA algorithm is used to communicate the location details of node, which will be used for the verification process. Simulation results show that our method yields accurate and faster results.**

Keywords — ***Cloud Networks, Encryption, Software agents, Location based services, VANET, Vehicular Cloud Computing.***

I. Introduction

Vehicular Cloud Computing (VCC) emerged as one of the solutions in order to address the issues in vehicular networks. Vehicles in VANET carry more resources than required such as communication system, on board facilities, storage, sensing equipment's etc. VCC uses these resources instantly to provide road safety and efficient traffic management. Details related to VCC like architecture, connection establishment, key management to provide secure communication link in vehicular network, security and privacy issues in VCC are discussed in detail in [1]. Most of the applications in vehicular cloud are based on location information which includes traffic status, emergency alerts and collision avoidance. Therefore, there is need to provide secure and reliable location information amongst the vehicles. This can be achieved in three ways. The active ways involve use of RADAR. Whereas in passive location integrity is achieved by achieved by filtering impossible locations and using assistance of neighboring vehicles. In this paper we present an agent based system which verifies the location of a node. This verification process involves a trusted party CA to which both the parties assent to for judgment. The CA has hidden verifier nodes in the network which have ample amount of resources required for the verification process such as storage, active location information gathering equipments such as RADAR and communicating capabilities with encryption algorithms embedded. These nodes appear as normal nodes for other entities in the network. Thus any node attacks targeted to harm the node or alter the location information sent by the node can be elevated, which increases the security of the location information. The addition of agent architecture in the proposed work draws all the advantages of the software agents. In terms of data analyzed, there is will be considerable reduction as number of verifier nodes are far less than the neighboring nodes which would be involved in the location verification process.

The VCC network considered for the proposed work is as shown in figure 1. The Vehicular Cloud (VC) is formed by the resources pooled by the Vehicle Nodes (VN), Cloud Service Providers (CSP), Road Side Unit (RSU) etc. All the activates are coordinated and monitored by a trusted entity called as Central Authority (CA). The CA is responsible for

DOI : 10.35291/2454-9150.2020.0681

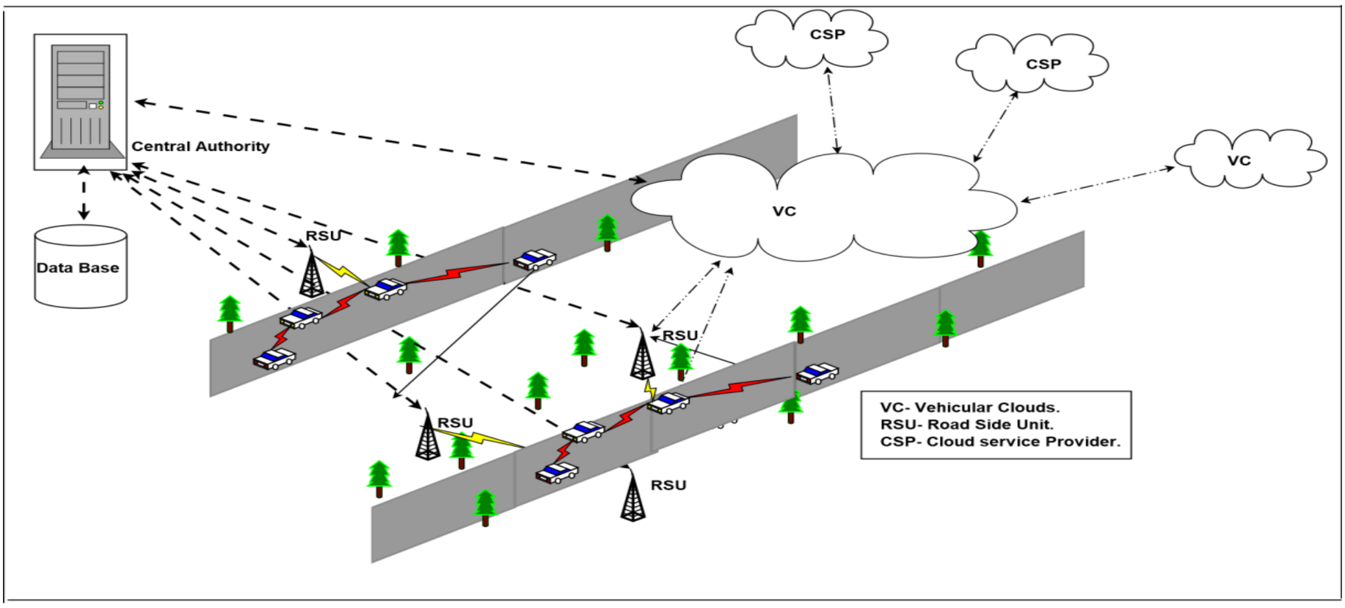

Fig 1: Vehicular Cloud Network

the following activities.

1. Registration of all the new vehicles.
2. Assign unique ID to each vehicle.
3. Generate public and private key pairs for verifier nodes.
4. Distribute the key pairs in a secured manner to the respective nodes.
5. Maintain DataBase (DB) with details of all nodes in the network.
6. Select verifier nodes and keep them in database with information such as location area they belong to , their public key.

Communications Links –

1. Vehicle nodes communicate using - vehicle to vehicle communication.
2. Vehicle nodes can also communicate with RSU- vehicle to infrastructure communication,
3. RSU communicates with CA, VC and local CSP's.

The paper is organized with Section 2 presents the related work, Section 3 presents the proposed RSA based location verification framework, Section 4 presents the simulation results followed by Section 5 with conclusion.

II. Related Work

In VANET the communication links established between the smart vehicles nodes and roadside units is unreliable and easily susceptible to attacks. A detailed literature survey on such methods of attacks and respective detection methodologies is presented in [2]. Important characteristics of VANET such as highly mobile nodes and dynamically changing network topology due to unpredictable node movements make it difficult to address the issues related to security. There is certainly a tradeoff between privacy and security. In order to execute security certain amount of information about the vehicle and vehicle user is necessary in case of any event, but protection of this data is also very crucial. There is continual increase in the number of vehicle users, more and more vehicle nodes add up to the VANET which demands for standardized security protocols. In real time the speed of vehicles may be faster than the threshold considered during simulation. Due to this high speed, links formed for communication between vehicles usually break more often. But the topology of VANET is more predicable than MANET. The VANET is dedicated to provide safety of the user. The response time for any event in VANET should be real time which otherwise leads to catastrophic, which will further attract attacks like Denial of Service (DoS). So, it is critical to prevent and detect the real time attacks. Further attack related to MANET and some specific to VANET are discussed which includes false position attack. Safety related services in VANET are highly dependent on reliable position related information. Disseminating false position data would give rise to reliability and security issues in VANET. In [3] VANET specific attacks, attacker model and challenges faced by the security methods for VANET's, requirements of security protocols and current observed solutions are presented in detail. The extension of conventional cloud computing in to the VANETs is presented in [4] by Prof. Olariu and his co-workers. The framework aims at providing the resources like storage, internet connectivity, infrastructure, traffic news, road conditions, intelligent navigation systems etc at an affordable cost to the other vehicles. The VC is divided in to Infrastructure-based VC and Autonomous VC (AVC). VC basically has three level services, which are application layer, platform layer and infrastructure layer. The user

DOI : 10.35291/2454-9150.2020.0681

chooses any of these based on application. In [5] security challenges specific to VC are presented. As VC is involving two different technologies i.e. cloud computing and VANET, the security and privacy issues related to both will be continuing in VC. But VC specific issues like scalability, single interface, confusing identities, ambiguous locations. More over trusting a node in case of high mobility in the presence of multiple nodes and short term communication link is a major challenge in VC. A detailed study on mobile cloud scenarios such as Mobile Vehicular Cloud, Mobile Personal Cloud, Mission Oriented Mobile Clouds is presented in [6]. Further the authors also discuss the application of mobile vehicular cloud namely Urban Surveillance service in the Vehicular Cloud, Vehicular Traffic Management. Connected vehicular cloud computing (CVCC) is a complicated technique which involves with telematics, vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I) communications, the integration of smart devices to provide numerous applications for the comfort of the users. This can be realized using applications such as Android Auto and Apple Carplay, which provide connectivity between car mobile apps with the social networking. But as the users connected increases the cyber security ricks also increase in a faster and more complicated manner which may lead to wrong decisions, hacking, injection of malware and virus which can easily corrupt the entire system. So it is crucial to provide strong secure environment by CVCC so as to be widely accepted and employed, which can be achieved with the involvement of vehicles and cloud service provider hand in hand. Motivated by the same a heterogeneous public good game (HPGG) to model is presented in [7] to take the security level higher.

The obstacle for exercising location based services is the lack of accurate and secure location verification systems. Due to which the location information is restrictively used only for security mechanisms. The location information is generated using the methods using signals from Global Navigation Satellite Systems (GNSS). But these signals may get manipulated by the malicious nodes if attacked. The functionality of SAGA using GPS and its features are presented in [8]. The author explains the attacks on the SAGA. The hidden signals in SAGA are generated based on secret code. In case if the attacker knows the secret code he is able to perform signal synthesis attack where he can generate valid location signals for any location he wants. If the attacker does not know the code then it tries to generate its own navigation signals and to match with the reference signal a hidden signal is inserted in the verifiers signal. Next attack is executed by delaying the incoming signals. But the damage caused would not be considerable if the all the signals are delayed with same amount of time. The only thing that needs to be done is resetting the synchronization signal which is possible only if transmitter and receiver are synchronized in time else they may receive an old signal and assume it to be fresh. If the signals are delayed for different time, then prediction of the position would be difficult. But to do so the signals needs to be separated which is extremely difficult as they are hidden in noise. Lastly in relay attack the attacker relays a valid location signal at location ‘v’ to attacker’s location. Longitude is location sharing protocol which preserves privacy of the users location and gives the control to user to decide who can access it [9]. The location data is encrypted by the secret key present with user using light weight encryption method. The overhead is reduced as the encryption of the data happens only once and the same is sent to nodes which are on the friend’s list of the user. This list can be revoked in accordance of the user without the consent of friend node.

A software agent is supreme self governing and self ruling agent which is capable enough to work as standalone process and perform actions without any assistance. It is responsive to the environment in which it is present and converse with user node as well as neighboring nodes. Sophisticated capabilities of software agents like reasoning, learning by incorporating the knowledge of the problem faced and planning to solve it makes it attractive for designers to implement large and complex systems with specialized agents[10][11].

In Greek crypto means hidden and graphy means writing. In cryptography readable data is converted to an unreadable format and vice-versa using one or two secret keys. In symmetric method same key is involved in encryption and decryption. Whereas in asymmetric method two different keys are involved, where one for encryption and one for decryption. RSA is asymmetric algorithm, the security of which relays on whose security depends upon the assumed difficulty which lies in factoring integers into their prime factors [12]. In data mining classification method categorize a sample to a particular specific item in a group of items. The training data set helps in development of the classifier model [13].

III. PROPOSED LOCATION VALIDATION SCHEME

In this paper we are presenting agent-based location verification system. Based on the literature survey, to our

DOI : 10.35291/2454-9150.2020.0681

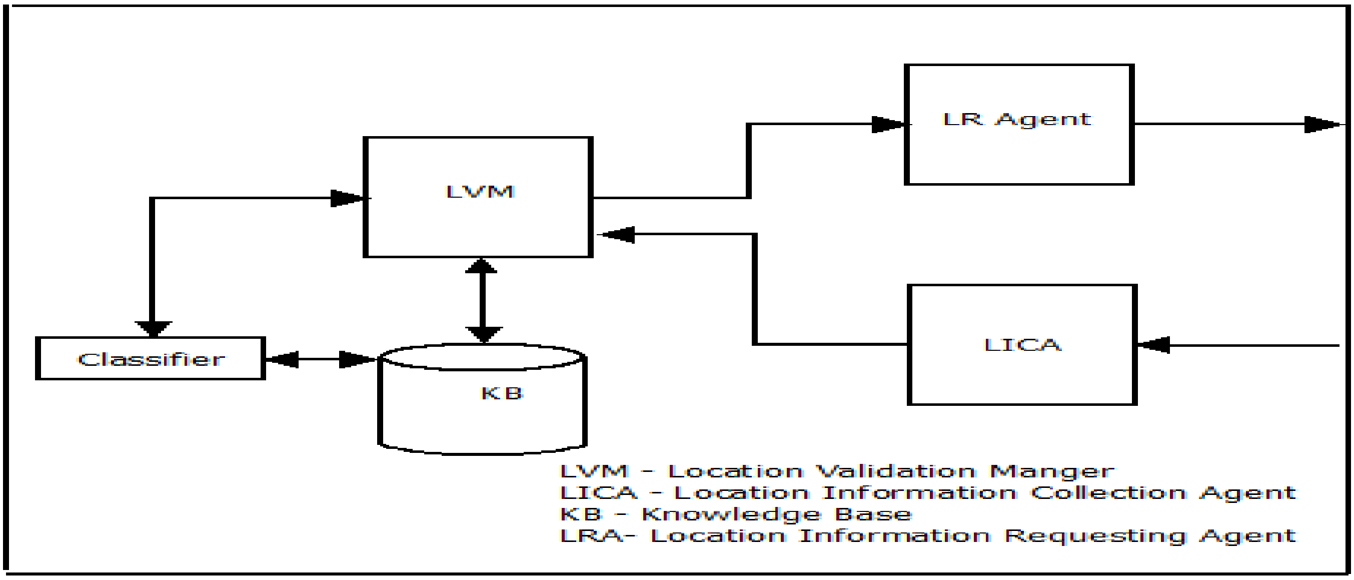
LR Agent
LVM
LICA
Classifier
KB
LVM - Location Validation Manger
LICA - Location Information Collection Agent
KB - Knowledge Base
LRA- Location Information Requesting Agent

Fig 2: Location Validation Agent.

knowledge there is no agent based mechanism to verify a location of a node using the hidden verifier nodes. The proposed scheme works as follows.

1. The verifier nodes are distributed randomly in the network.
2. The presence of verifier nodes is known only to the CA.
3. To other nodes in VC the verifier nodes appear as normal nodes.
4. The Location verification agency is installed in CA.
5. In case of dispute the CA triggers the location verification agency.

The location verification agency consists of location verification manger, Knowledge base and location verification data collection agent.

Location Verification Manager (LVM): It coordinates all the activates of the agency. When a dispute arises, the Agency is triggered by CA. The CA sends information of vehicle node whose details need to be cross verified along with details such as location, time etc. LVM searches its data base KB for the verifier node list. LVM send message regarding location verification to the verifier nodes as in eq 1.

$$Loc_{req} = Vpuk\ [Message[ID|Time] \qquad (1)$$

Where Vpuk- Public key of verifier node

Eq 1 can be decrypted only using private key of verifier node. The verifier nodes respond to Locreq. They search the database and search for the vehicle ID. If found it sends the time of encounter and location as shown in eq 2.

$$Loc_{res}= CApuk[Message[Message[ID|Time]|\ ID|Time|loc]] \qquad (2)$$

Where CApuk- Public key of CA.

Else they do not respond. This makes considerable reduction in the number of messages to be processed by the LVM. Eq 2 can be decrypted only by the private key of CA.

Location Request Agent (LR agent) : This is triggered by LVM to forward the location request message to the verifier nodes.

Location Information Collection Agent (LICA): The response from the verifier nodes is collected by the LICA and provided to LMA. The LICA is triggered by LVM.

Knowledge Base (KB): The database of all the vehicle nodes, their key pairs etc. KB is frequently updated by output of classifiers, LVM.

Classifier: The classifier decides whether or not the vehicle was present in a particular location at particular time. Classifier decides location of the node based on the data from LVM and KB.

A. RSA encryption decryption algorithm

The RSA Algorithm works as follows when a message is to be transmitted securely to destination.

Step 1	Choose two large distinct primes p and q. Form the public modulus $n = pq$.
Step 2	Choose public exponent e to be coprime to $(p - 1)(q - 1)$, such that $1 < e < (p - 1)(q - 1)$.
Step 3	The pair (n, e) is the public key.
Step 4	The private key is the unique integer $1 < d < (p - 1)(q - 1)$ such that $ed = 1 \bmod (p - 1)(q - 1)$.

Table 1: RSA Algorithm Steps

Encryption : The message to be encrypted is 'M'. Usually if the size of the message is large it is divided in to small chunks each of same size. The encryption of the message 'M' is done using the public key of the destination as shown in eq 3.

DOI : 10.35291/2454-9150.2020.0681

$$C \equiv E(M) \equiv M^e (\mathrm{mod}\ n) \qquad (3)$$

Decryption: When the cipher text ‘C’ is received by the destination it is decrypted using its private key as shown in eq 4.

$$D(C) \equiv C^d (\mathrm{mod}\ n) \qquad (4)$$

The encryption key - Pair of positive integers (e; n). The decryption key - Pair of positive integers (d; n).

The sequence of working steps of the proposed location validation framework is as follows.

1. CA gets the query on location information of vehicle node ‘A’ at given time and location claimed by the vehicle node ‘A’ of its presence. This is forwarded to Location Validation Agent (LVA).
2. Location Validation Agent (LVA) checks its database and find the list of verifier nodes in that location region.
3. Location Validation Agent (LVA) triggers LR agent and sends location request as in eq 1.
4. This message is decrypted by verifier nodes using their respective secret key.
5. The verifier node checks its database for encounter of the vehicle using ID details sent in request message by CA.
6. If not encountered in its region the verifier node does not respond. Else location details are encrypted using public key of CA and sent as in eq 2.
7. The LICA collects these messages and provides it to LVM.
8. LVM forwards details such as collected location messages from verifier, Location etc. claimed the classifier.
9. The outcome of the classifier decides whether or not the vehicle node was present in the location claimed.

IV. Results

Simulation of the proposed work is done in C++ language. A plot of Number of vehicle node to Time taken by the network to configure is shown in fig 3. We can observe there is increase in the time taken by the network to configure as the number of nodes increases. The increase in the time is due to involvement of more highly mobile nodes. RSA is asymmetric algorithm which involves a pair keys - private key and public key associated with each entity. The time taken for the generation of key pair versus number of bits considered in the key is shown in fig 4. Due to complexity in the key generation as explained earlier, time taken to generate the keys increases as the number of bits involves increases. Entropy is the amount of randomness in the information. Higher the value of entropy in data, higher is the randomness and uncertainty in predicting the future. It is appreciable is entropy of cipher text is high. Figure 5 shows the plot of entropy of cipher text generated by different encryption algorithms for the same plain text. It can be seen that the entropy of cipher text generated by proposed RSA based location verification method is high compared to other standard methods.

Figure 6 presents the variation in the decryption delay for change in the number of bits in the key for different sizes of data. We can observe that the time required for decrypting the data increases with increases in message size that is to be decrypted and number of bits used in the key. Entropy represents the level of randomness in the text. Higher the level of entropy in the cipher text better is the encryption algorithm. In fig 7, we can observe that the RSA provides better entropy as the key size goes on increasing. Figure 8 represents the scenario where time taken by the CA to decrypt the received message ‘C’ is plotted versus number of bits in the key for different size of data chunks.

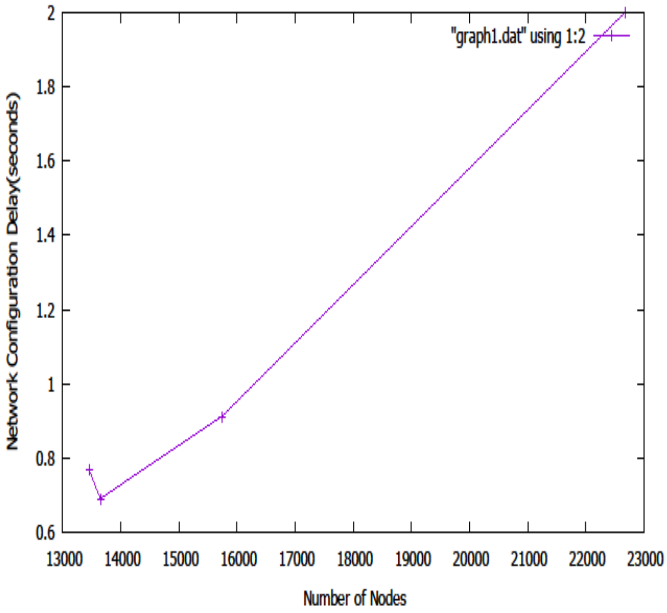

Fig 3: Network Configuration Delay Vs. Number of nodes

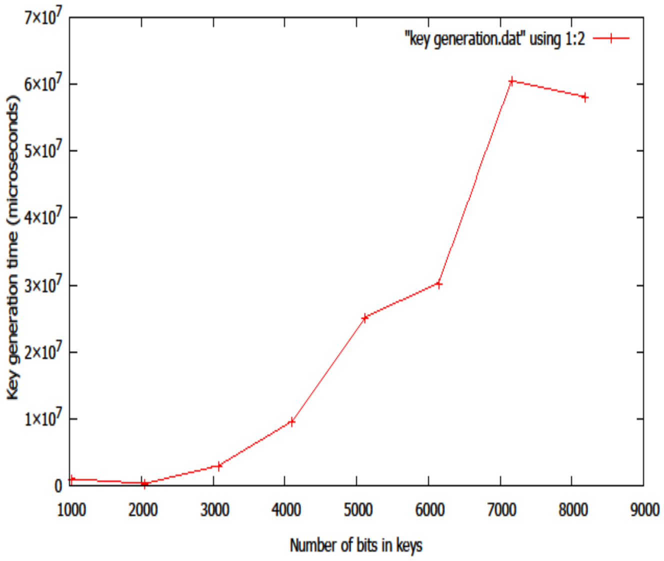

Fig 4: Key generation time Vs. Number of bits in key

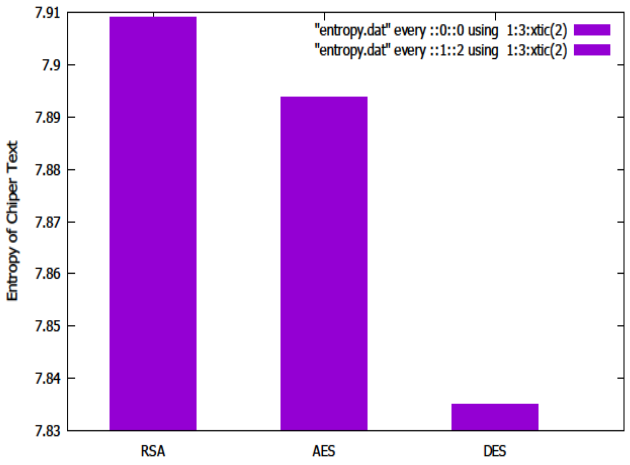

Fig 5: Entropy of cipher text Vs. Encryption Algorithms

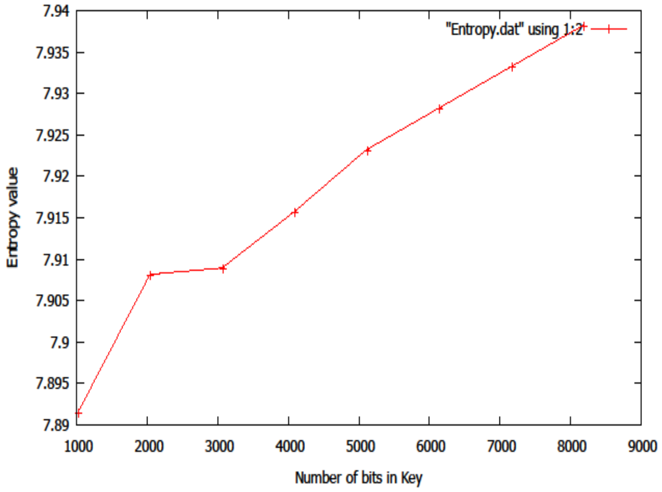

Fig 6: Entropy of cipher text Vs. Number of bits in the key

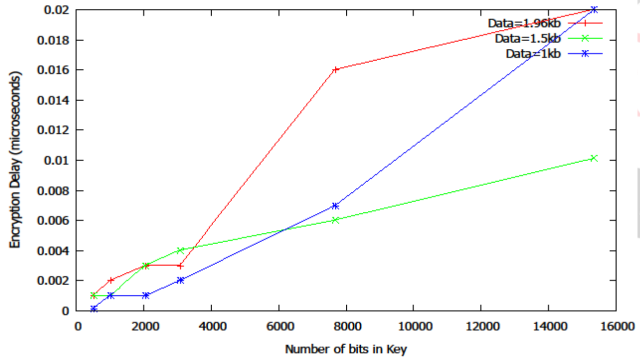

Fig 7: Encryption Delay Vs. Number of bits in key

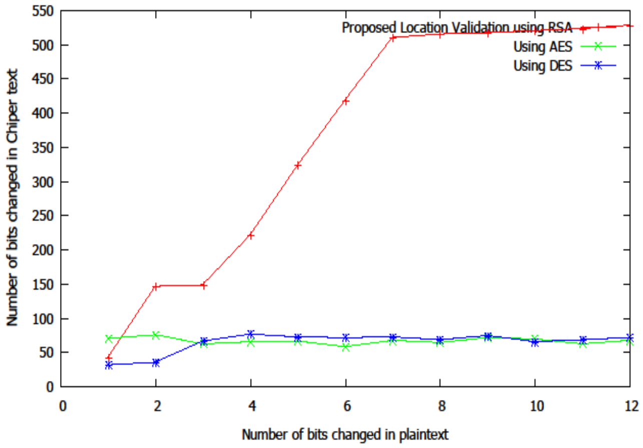

Fig 8: Avalanche effect for different encryption algorithm

We can observe that there is more decryption delay for keys with more and more bits. It can also be observed that the Increase in the data size also increases the delay. Avalanche effect is the change in the number of bits in cipher text to the number of bits changed in the corresponding plain text. It is appreciable if the encryption algorithm produces good avalanche effect. In fig 9 it can be observe that the proposed Location validation based on RSA encryption algorithm presents good avalanche effect as compared to AES and DES encryption algorithms.

In location based services the role of location information of nodes plays a vital role. It may be a alerting message containing the location of vehicle node which has met with accident or a node accessing VC privileges which are based on geographical location of a node.

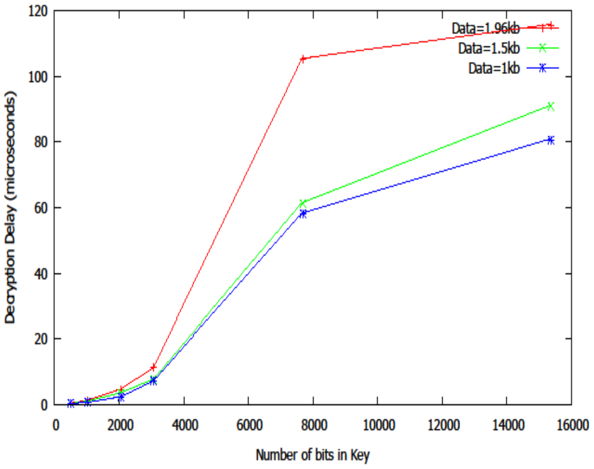

Fig 9: Decryption Delay Vs. Number of bits in key

If this location information gets hampered then purpose of the service entirely demolishes. Thus the encryption algorithm should be strong enough to withstand the attacks by the malicious nodes. Observing the results the proposed location validation frameworks produces good results in avalanche effect and entropy of the cipher text. Thus if the attacker has ample amount of information related the secret key, it will not be sufficient enough to break in to the message. As the key size increases the encryption delay, decryption delay key and generation delay increases. So the size of the key plays important role in deciding the time taken for validation. But there is tradeoff between security and number of bits in the key. So the size of the key should be chosen wisely.

V. CONCLUSION

Location information is vital in location based services. Most of the applications of cloud computing are based on location information of the node which may be used for service delivery. Malicious nodes may attack this location information in order to avail services which they are allocated and may deny later. Our frame work presents an agent based secured location verification method using RSA to solve this issue. The location information is cross checked by the help of hidden verifier nodes known only to

DOI : 10.35291/2454-9150.2020.0681

CA which are distributed in the network. Our simulation results show that the proposed framework gives better performance in terms of entropy and avalanche effect which are crucial for any encryption involved method.

REFERENCES

[1] Whaiduzzaman, M., Sookhak, M., Gani, A., & Buyya, R." A survey on vehicular cloud computing". *Journal of Network and Computer applications*,2014, pp 325-344.

[2] Sakiz, F., & Sen, S. "A survey of attacks and detection mechanisms on intelligent transportation systems: VANETs and IoV". *Ad Hoc Networks*, pp 33-50, Aug. 2017.

[3] Samara, G., Al-Salihy, W. A., & Sures, R.," Security analysis of vehicular ad hoc nerworks (VANET)". In *2010 Second International Conference on Network Applications, Protocols and Services*, (pp. 55-60), May 2010.

[4] M. Abuelela and S. Olariu "Taking vanet to the clouds " *Proceedings of The 8th International Conference on Advances in Mobile Computing and Multimedia MoMM*, pp. 8-10, Jun. 2010.

[5] A. Friedman and D. West "Privacy and security in cloud computing " The Centre for Technology Innovation: Issues in Technology Innovation no. 3, pp. 1-11, Sep.2010 .

[6] M. Gerla, "Vehicular Cloud Computing," 2012 The 11th Annual Mediterranean Ad Hoc Networking Workshop (Med-Hoc-Net), Ayia Napa, pp. 152-155, Jan. 2012.

[7] A. Alamer, Y. Deng, G. Wei and X. Lin, "Collaborative Security in Vehicular Cloud computing: A Game Theoretic View," *IEEE Network*, pp. 72-77, Jul. 2018.

[8] Becker G.T., Lo S.C., De Lorenzo D.S., Enge P.K., Paar C. Secure Location Verification. In: Foresti S., Jajodia S. (eds) Data and Applications Security and Privacy XXIV. DBSec 2010. Lecture Notes in Computer Science, vol 6166. Springer, Berlin, Heidelber, pp 366-373, Dec. 2010.

[9] Dong, C., & Dulay, N." Longitude: A privacy-preserving location sharing protocol for mobile applications". In *IFIP International Conference on Trust Management* Springer, Berlin, Heidelberg, pp. 133-148, Jan. 2011

[10] Abar, S., Theodoropoulos, G. K., Lemarinier, P., & O'Hare, G. M.. "Agent Based Modelling and Simulation tools: A review of the state-of-art software". *Computer Science Review, 2017*, pp 13-33.

[11] Kittali, R. M., Mahabaleshwar, S. K., & Sutagundar, A. V. (2016, October). "Congestion controlled adaptive routing in wireless sensor network". In *2016 International Conference on Signal Processing, Communication, Power and Embedded System (SCOPES)*, pp. 1528-1532, Jun. *2016*,.

[12] El-Deen, A., El-Badawy, E., & Gobran, S. (2014). "Digital image encryption based on RSA algorithm". *J. Electron. Commun. Eng*, pp 69-73, May 2014.

[13] Adebayo, A. O., & Chaubey, M. S. (2019). "Data mining classification techniques on the analysis of student's performance". *GSJ*, pp 45-52,Aug. 2019.

DOI : 10.35291/2454-9150.2020.0681