Secured VANET Protocol with signature authentication (SVPSA)

Sonia Lal
Dept. of CSE
Uttarakhand Technical University
Dehradun, India

Anshika Goyal
Dept. of CSE
Uttarakhand Technical University
Dehradun, India

ABSTRACT
Vehicular Area Network (VANET) plays an important role in today's demand of smart roads where the traffic needs to be monitored for safe commuting along with it, the commuters should also be given facilities in case of an emergency or otherwise. Keeping in mind the challenging requirements of the present and the future, in this paper work first previous solutions were reviewed and a new Secured Protocol for VANET with Signature Verification has been proposed. Modified Hill cipher and RSA algorithms are used in sequence to secure the Vehicle's information transmitted to the Road Side Unit(RSU). Signature verification has been taken care of using Baker's map. MD5 hashing has been also used to ascertain that there was no intrusion. The device in the vehicle and the RSU communicates only when the signatures are verified. A comparative analysis has also been presented where it has been observed that the proposed algorithm performs better than simple RSA algorithm. The results obtained shows an improvement in Bandwidth by 16%, energy consumed is reduced by 14% and time reduced by 5%. The results indicate that the proposed method not only secures the privacy of the commuters but also uses lesser resources. It can be concluded that the proposed three tier secured structure is more robust than the existing models.

Keywords
VANET, RSU, RSA, MD5, Hill Cipher, Signature verification

1. INTRODUCTION
Vehicular Ad hoc Network (VANET) is a specially designed system which utilizes IEEE 802.11a/g/n standards of wi-fi, though many new protocols and models have come up to fine tune the network. In light of the major ideas of these systems, a few different classes have risen, for example, remote work systems, remote sensor systems, Mobile Ad-hoc Networks(MANET). VANET is a developed structure of MANET where every hub (vehicle) moves unreservedly inside the system scope region. In VANE, every vehicle goes about as a switch to trade information between vehicles in the system. VANET helps the drivers to not only navigate over a stretch but also helps them to put in their service requests in case of emergency or otherwise also, VANET provides the drivers an Intelligent Transportation System(ITS) administrations during their drive, for example, street wellbeing, effective driving, service request like out of gas or accident or even very minor requests, and also infotainment to the end users[1,2].

VANET utilizes vehicles as hubs to frame a versatile impromptu system for the scattering of security and giving administrations on a call. It has been intended to offer an abnormal state of wellbeing for the drivers with a specific end goal to limit various streets mishaps. With each new mechanical applications particularly PCs and system applications, comes new security challenges. Each system in present day is defenseless to security assaults and VANET is no exemption. With a great many vehicles employing on the national and state streets the interest for administrations likewise increment. The street systems like eastern, western and focal fringe would be required to be all around prepared to give administrations to the suburbanites as there is not really any living space. Fast on national roadways is inclined to mishaps and break downs. Blasting of tires is most normal, coming up short on fuel with no oil station in 5-10 kms would be a testing situation for the commuters. Albeit current vehicles carry few dynamic capabilities life auto navigation, sensors, cameras, but auto collisions are even an unremarkable unavoidable truth. Indeed, even with the present wellbeing highlights, insights demonstrate that constant flows of accidents keep on occurring. A considerable lot of these mishaps or accidents could possibly be forestalled or maintained a strategic distance from if pre-crash admonitions were accessible to the drivers. The authors have proposed a new secured protocol for VANET to meet out the present need of secured and effective transmission of data over the network for secured movement of the vehicles on the road.

2. RELATED WORK
Over the years reserachers have proposed various protocols and models for VANET implentation and security. Prevention from Illusion assault [3] in 2009 was presented, where an aggressor purposefully deceives on his/her vehicle to deliver wrong sensor readings. Same year [4] proposed HEAP to identify the Wormhole assaults in the AODV convention of VANETs, which is a change of beforehand proposed parcel rope strategy [5]. In th same year [6] a timestamp arrangment was proposed to counter the Sybil assault. In 2010 [7] a circulated security approach was proposed which could discover Sybil hub.The approach functioned admirably in a huge system however in little scale systems, it gave all the more false positive rates. In 2011[8] a disperse and vigorous way was proposed to counter Sybil attack.In the proposed approach, every hub kept a record of its neighboring hubs and additionally trade gatherings of its neighboring hubs intermittently and played out the crossing point of these gatherings. The approach was not able to recognize the Sybil hubs in the situation where the assault length wasshorter than the predefined edge esteem. In 2013 [9] A Wormhole Attack Detection Protocol utilizing Hound Packet(WHOP) which depended on AODV was proposed. The convention had higher recognition rate yet the issue was that it additionally amplified the preparing postponement of the bundles. In the same year [10] prevention from Denial of Service(DoS) assault was proposed. The downside of the apporach was that it failed during heavy traffic situations which is expected on

the busy high-ways. In the same year [11] a method called BAMBi to identify Black Hole hubs in the system was proposed. Because of the high versatility of vehicles, this procedure is too overwhelming to send and isn't practical in VANET. In 2012 [12] a model to break down the effect of the Black Hole assault was proposed in which a pernicious hub puts on a show to have an ideal course for the goal hub, sends counterfeit directing data and demonstrates that bundle should course through this hub. In the same year [13] proposed a pre-verification plot that recognizes Denial of Service assault propelled by an untouchable assailant. In the same year [14] proposed a system to identify and anticipate Sinkhole assaults in the system. This instrument comprised of four stages: Initialization, Storage, Investigation and Resumption. In 2013 [15] proposed an effective way to deal with identify and shield against UDP flooding which is a typical class of DoS assaults under various IP mocking. In the same year [16] proposed an Attacked Packet Detection Algorithm (APDA) that distinguishes DoS assaults before confirmation time. In 2015 [17] proposed to anchor VANET utilizing Wi-Fi-IEEE 802.11p. They proposed to evacuate getting out of hand or pernicious hubs utilizing trust level. The plan gave classification and honesty of the messages. In the same year [18] recommended that VANET was rising as a noticeable type of MANETs and as an astounding science for providing a broad scope of insurance applications for auto travelers. In the same year [19] assessed the country of the craft of security protecting plans for advert hoc informal organizations comprising of versatile interpersonal organizations(MSNs) and vehicular interpersonal organizations (VSNs). In 2016 [20] proposed a half breed anchored structure for VANET. The consolidated RSA and AES calculations to produce a cross breed plot for anchoring the vehicle correspondence in VANET. In the same year [21] recommended that Vehicular informal organization (VSN) is foreseen to fill in as a basic measurements detecting, trading and preparing stage for the future Intelligent Transportation Systems. They proposed to handle the region security trouble in VSNs. In the same year [22] broke down that Cryptographic natives were vital building hinders for outlining security conventions to obtain classification, verification, uprightness and non-denial. In 2017 [23] recommended that Cryptography was a way to deal with secure data from gatecrashers. It gave guarantee, as well as gave credibility. Altered approach which was an improvement over customary RSA calculation by including exponential forces, n prime numbers, various open keys, and K-NN calculation was proposed.

3. RESEARCH METHODOLOGY

3.1 Parameters used to Analyze Proposed Algorithm

Following are the three parameters used for analysis purpose:

(1) **Bandwidth Consumed**: It describes maximum data transfer rate of a network on connection. It measures how much data can be sent over a specific connection in a given amount of time.

- **Required Bandwidth**

$$\boldsymbol{rb} = \left(\frac{\boldsymbol{bw}-\Delta\boldsymbol{b}}{\boldsymbol{n}}\right) \qquad \textbf{(i)}$$

Here bw is the initial bandwidth,Δb is change in bandwidth. n is number of nodes.

- **Consumed Bandwidth**

$$\boldsymbol{BW} = \sum_{i=1}^{n} \boldsymbol{rb_i} \qquad \textbf{(ii)}$$

BW is total bandwidth.

(2) **Energy:** This shows the performance of cryptography algorithm in terms of energy consumption for encryption and decryption process.

- **Energy requirement**

$$\boldsymbol{re} = \left(\frac{\boldsymbol{E}-\Delta\boldsymbol{E}}{\boldsymbol{n}}\right) \qquad \textbf{(iii)}$$

E is the initial energy, ΔE is the change in energy.

- **Total energy consume**

$$\boldsymbol{Te} = \sum_{i=1}^{n} \boldsymbol{re_i} \qquad \textbf{(iv)}$$

n is number of nodes. Te is total energy.

(3) **Time:** This parameter shows the time taken by the algorithm in encryption and decryption process.

- **Total time consumed**

$$\boldsymbol{Time} = \sum_{i=1}^{n} \boldsymbol{et_i} - \boldsymbol{st_i} \qquad \textbf{(v)}$$

n is number of nodes, et is the end time and st is start time , time is the total time consumed.

3.2 Implementation

Setup

Protocol - 6LoWPAN
MAC layer – IEEE 802.15.4
Frequency – 2.4 GHz
Bandwidth – 250 kbps
Power – 1 mw radio (mega watt)

The proposed approach Hill Cipher calculation and RSA calculation are changed for encryption reason. The encryption part of Hill Cipher takes m progressive plaintext letters and it produces m ciphertext letters. Keeping in mind the end goal to get ciphertext letters, n direct conditions are utilized as a part of which each character of both plaintext and ciphertext is appointed a numerical incentive as a=1, b=2, c=3,… , z=26. In Hill Cipher, a network containing numbers called encryption key lattice which is utilized for encryption process and the particular number-crunching backwards of the encryption grid called unscrambling framework is utilized in decoding process.Thus, in the Hill Cipher the means required for encryption and unscrambling are given by C = KP mod 26 and P = K-1 mod 26where P is plaintext, K is the encryption key framework, C is the ciphertext and K-1 is the measured math opposite of K i.e., decoding key grid. In Hill Cipher to perform encryption, the key encryption key matrix(K), called key lattice ought to be chosen such that it must fulfill two essential criteria viz., the key grid must be invertible and regardless of whether is invertible, the gcd (det(K), 26) must be 1, at that point just decoding network is conceivable. It is noticed that the key framework is arbitrarily picked and in numerous circumstance the picked key lattice isn't fulfilling said criteria.

L value is an extension to original hill cipher algorithm. This value is subtracted for encryption and added for decryption process. Each letter is represented by a number modulo 256. To encrypt a message, each block of n letters is multiplied by an invertible n × n matrix, against modulus 256. To decrypt the message, each block is multiplied by the inverse of the matrix used for encryption.

The encrypted message is then passed on to the modified RSA. The two random numbers taken are generally 8 bit but in the modified algorithm the numbers are converted into 64 bit first, phi is calculated by multiplying the two prime numbers after converting them to even, which is not the case in conventional RSA, gcd of phi and a randomly generated integer is calculated until gcd is not equal to 1 or randomly generated number is not equal to 0. This is followed by and additional loop which is not present in the conventional RSA. The loop runs till true, within the loop a value d is increment each time and modulus of d and randomly generated number is calculated against phi. At the end of the loop public and private keys are received. The signatures are generated using Baker's map. The signatures generated at sender aspect referred to as signer and additionally at receivers facet referred to as verifier. To ascertain that no tempering has been done with the data MD5 hash code is also generated at receiver and sender end. If these don't match then it would suggest that the message has been tempered.

Algorithm
Step 1. Take owner detail
Step 2. Use modified hill cipher to encrypt the message
Step 3. Modified RSA Algorithm
Step 4. Match h and h1
Step 5. Match signer's and verifier's signature
Step 6. If matched that means the message travelled safely.

3.3 Psuedocode

Initialize L value (assume L value, have taken 65 since 65 is ASCII code of A)
modulo ←256 (modulo is a number required to calculate the modulus generally it is 26)
OMD5 ← get md5 of the original message
C← Convert the message to ASCII and subtract L value from it
n ← calculate no of iterations using
col ← get number of columns of the message (since matrix is linear)
divide col into half
n ← col/2
k←generate a 2 X 2 random key
loop from i←1 to n
y ← multiply C(i) by k
get modulo of yt ← (y,modulo)
end loop
EnMsg ← yt+L; (add L value to encrypted message)
p,q ← get two prime numbers
convert the numbers to 64 bit
prod←get the product of p and q
phi ←get euler totient
generate public and private key
loop till gcd of euler's totient is not equal to 1 or a prime number is not detected
n1 ← get random number based on product
e← get random number based on n
check if e is prime (would return one if e is prime on 0 loop will terminate)
get gcd of e and phi
end loop
Baker's Map Applied on the data received
d←0
loop till mod of d and phi not equal to 1
d←d+1
val ← mod(d*e,phi)
end loop
loop while **i** does not reaches end of message
m←message(i)-L
qm← convert e to binary
len←length(qm)
c←1
loop till **ii** reaches end of qm
if(qm(ii)=='1')

c←mod(mod((c^2),prod)*m,prod);
elseif(qm(ii) equal to zero) then
c←(mod(c^2,prod));
end if
end loop
c1(i)←c
qm1←dec2bin(d)
len1←length(qm1)
nm←1
ii←1
loop till ii not equal to len1
if(qm1(ii) is equal to '1') then

nm←mod(mod((nm^2),prod)*c,prod)
elseif(qm1(xy) is eual to '0') then
nm←(mod(nm^2,prod))
end
ii=ii+1
end loop
nm1(i)←char(nm+32)
i←i+1
end loopproposed Algorithm
RMD5 ← get MD5 of the received message after decryption
If RMD5 is equal to OMD5
Display "Signatures match"
else
Display "Unauthorised user"
End

Table 1. Notations used

Notation	Description
c1	Encrypted message
H	MD5 hash code of c1
nm1	Decrypted message
h1	MD5 hash code of nm1
qm	Length of the message
Prod	Product
C	Variable(value 1)

4. RESULT AND ANALYSIS

4.1 Snapshot for Proposed algorithm

Figure 1 shows vehicle being recognized by the RSU after recognizing the object, the connection is established as soon as the vehicle comes into contact.

Figure1: Shows Vehicle detected by the RSU

Figure 2. shows the path of the vehicles being traced by the RSU to know the location information and smooth movement of the vehicle. Shows vehicles being traced

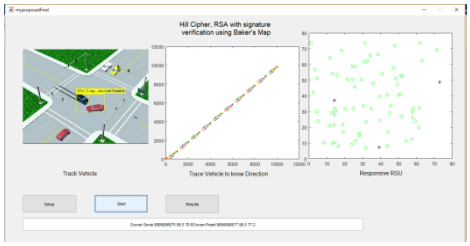

Figure 2: Shows vehicles being traced

Figure 3. shows request received by the RSU once the connection is established between the vehicle and the RSU. The priority of the requests is also marked. The proposed model considers Low, High, Urgent and Emergency(marked as A) as the priority levels.

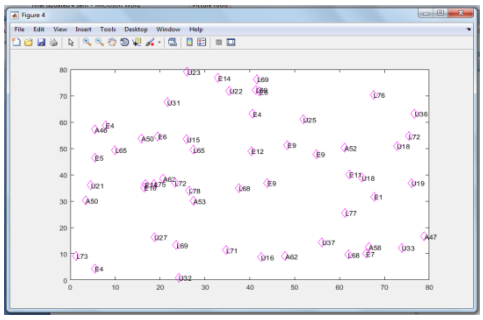

Figure 3: Consumption of Bandwidth

From figure 4 we can conclude the bandwidth consumption of the proposed model is much lesser than standard RSA model. The proposed model was able to save 16% bandwidth. The proposed model is able to maintain the bandwidth consistently throughout and that the consumption is much lesser than the standard RSA algorithm under the same scenario. Nodes represents the device in the vehicles

Energy Consumption

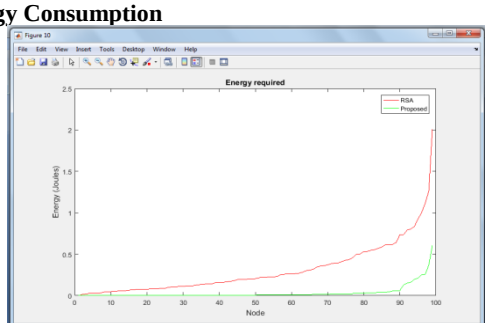

Figure 4: Energy consumed

Time

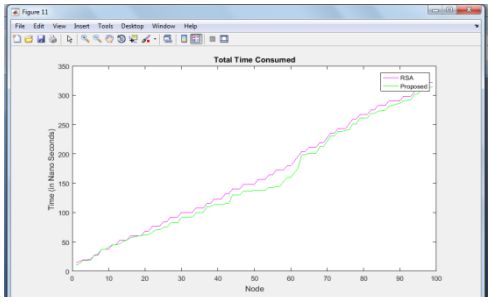

Figure 5: Time Consumption Plot

As can be seen from the following graph figure 6 time taken by the proposed approach is lower than RSA algorithm. It also shows the progress of the time consumed with passing of vehicles and the total time consumed. It is observed that the time consumed by the proposed algorithm is 5% lesser than the existing RSA algorithm.

4.2 Qualitative comparison of Proposed Algorithm and RSA on different parameters

Table 2 shows the qualitative analysis of the proposed and the standard RSA algorithm in terms of different constraints. The observation indicated that the proposed algorithm outperforms the standard RSA algorithm.

Table 2: Qualitative Comparison

Parameters	**Proposed algorithm**	**RSA algorithm**
Objective	Secure personal information of the vehicle Establish secured connection Verify authenticity of data	Secure data Verify received data
Security	Two level security based on Reputation and Observation.	Single level security designed on reputation.
Design Consideration	Design to be executed on 6LoWPAN capable of communicating with 802.15.4 devices.	Designed on 802.11a/g
Adaptation to Topology changes	Adaptation is good as the protocol is flexible.	Average adaptation
Scalability	Minimum overhead	Average overhead
Packet Overhead	Minimum overhead	Average overhead
Processing	Very Low processing	Low processing

4.3 Quantitative Comparison of Proposed Algorithm and RSA

Table 3 shows the quantitative analysis of the proposed and the standard RSA algorithm on different parameters. From table we can conclude that the bandwidth is improved by 16%, energy consumed is reduced by 14% and time taken is also reduced by 5%.

Table 3: Quantitative comparison

Parameters	Percentage
Bandwidth Consumption	16%
Energy Save	14%
Time Taken	5%

5. CONCLUSION

VANETs are of an increasing importance as they enable accessing a large variety of ubiquitous services. Such increase is also associated with a similar increase in vulnerabilities in these inter-vehicular services and communications, and consequently, the number of security attacks and threats. The successful defending against such VANETs attacks prerequisite deploying efficient and reliable security solutions and services. This paper has provided, discussed, and analyzed the VANET issues, security requirements. Among all requirements privacy is the major issues in VANET. To secure our network from attackers who intercepts the signature and messages and modifies it, in this thesis we are using an algorithm which is Hill Cipher algorithm and RSA algorithm which are modified and Bakers map and MD5 are used for signature verification. The proposed approach is compared with RSA algorithm on different parameters like bandwidth consumption, energy consumption and time taken. The results obtained show that the bandwidth is improved by 16%, energy consumed is reduced by 14% and time taken is also reduced by 5%. Hence the secured framework using modified RSA and Hill Cipher algorithm is better and efficient than RSA.In future the model can be tested over cloud and predictive modelling may also be tried using Machine Learning(ML).

6. REFERENCES

[1] Toor, Y., P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues". Communications Surveys & Tutorials, 2008, IEEE. 10(3): pages 74 to 88.

[2] Jerbi, M., "Vehicular Communications Networks: Current Trends and Challenges". 2010, Global IGI: pages 251 to 262.

[3] Lo, N. W., & Tsai H. C., "Illusion attack on VANET applications-A message plausibility problem",. 2007, IEEE, Globecom Workshops.

[4] Safi, S.M., A. Movaghar, & M. Mohammadizadeh, "A novel approach for avoiding wormhole attacks in VANET", 2009, IEEE, AH-ICI.

[5] Hu, Y.-C., A. Perrig, & D.B. Johnson. "Packet leashes: a defense against wormhole attacks in wireless networks", 2003 INFOCOM 2003, IEEE, 22nd Conference on Computer and Communications.

[6] Park, S., "Defense against sybil attack in vehicular ad hoc network based on roadside unit support", 2009, IEEE, MILCOM.

[7] Grover, J., M.S. Gaur, & V. Laxmi, "A novel defense mechanism against sybil attacks in VANET", 2010, 3rd ACM.

[8] Grover, J., "A sybil attack detection approach using neighboring vehicles in VANET", 2011, 4th ACM.

[9] Gupta, S., Kar, S., & Dharmaraja S., "WHOP: Wormhole attack detection protocol using hound packet", 2011, IEEE, IIT.

[10] Sumra, I.A., "Classes of attacks in VANET", 2011, IEEE,Electronics, SIECPC.

[11] Misra, S., K. Bhattarai, & G. Xue. BAMBi: "Blackhole attacks mitigation with multiple base stations in wireless sensor networks", 2011 IEEE, ICC.

[12] Al-kahtani, M.S.,"Survey on security attacks in Vehicular Ad hoc Networks (VANET)",2012,6th, ICSPCS .

[13] He, L. & W.T. Zhu.,"Mitigating DoS attacks against signature-based authentication in VANETs", 2012, IEEE,Internation conference, CSAE.

[14] Gandhewar, N. & R. Patel. "Detection and Prevention of Sinkhole Attack on AODV Protocol in Mobile Adhoc Network", 2012, IEEE, 4th international conference, CICN.

[15] Verma, K., H. Hasbullah, & A. Kumar. "An efficient defense method against UDP spoofed flooding traffic DoS attacks in VANET". 2013, IEEE, 3rd IACC.

[16] RoselinMary, S., M. Maheshwari, & M. Thamaraiselvan. "Early detection of DOS attacks in VANET using Attacked Packet Detection Algorithm(APDA)". 2013, IEEE, ICICES.

[17] Thanmayee Karimireddy, Ahmad Ghulam & A Bakshi, "A hybrid security framework for the vehicular communications in VANET", 2016, IEEE, WiSPNET, 2016, 10.1109/WiSPNET.2016.7566479.

[18] Bariah L., Shehada D., Salaha E., "Recent advances in VANET security: a survey", 2015, 10.1109/VTCFall.2015.739111

[19] L. M. Ibrahim, "Social networks: Privacy issues & precautions", 2015, 9th Int. Conf. Digit. Soc. (ICDS), pages 65 to 69.

[20] Jiri Fridrich. "Secure image ciphering based on chaos", 1997, AFRL, New York, USA.

[21] Yu R., "MixGroup: Accumulative pseudonym exchanging for location privacy enhancement in vehicular social networks", 2016, IEEE,vol. 13, no. 1, pages 93 to 105.

[22] Shim K. A., "A survey of public-key cryptographic primitives in wireless sensor networks", 2016, IEEE, vol. 18, pages 577 to 601.

[23] Shikha Mathur, "Analysis & design of enhanced RSA algorithm to improve the security", 2017, ICCT 17029536