Security Issues and ANALYSING Sybil Attack Detection in VANET

K.Selvakumar, S.Naveen Kumar

Abstract*: *As of late, the quantity of vehicles on the road has expanded tremendously. Because of high thickness and portability of nodes, conceivable dangers and road accidents are expanding. Wireless communication permits sending safety and other basic data. Vehicular Ad-Hoc Network (VANET) is an innovation which accommodates the vehicle as node to interconnect with each other through a wireless network. The essential structure goal of these applications is to serve the clients and give security of human lives amid their journey. Security is a major issue in VANET as it can be life threatening. We propose ECEDS (Elliptic Curve Encryption and Digital Signature) gives system security by utilizing a digital signature for message communicated over the system. This framework likewise used to counteract Sybil attack by limiting timestamps given by RsU at a beginning stage itself. An attacker is one of sort of end client, yet their role in the system is negative and makes issues for different segments of system. A serious attack, known as Sybil attack, against ad-hoc networks includes an attacker misguidedly asserting numerous characters. A Sybil attack delivers different messages to different nodes. Every message contains distinctive source personality. In this paper, we discusses some of the techniques put forwarded by researchers to detect Sybil attack in VANET. In this paper, we propose a Preference Batch Authentication Algorithm (PRBAA) expecting to decrease the message loss rate of nodes and Road-side Units (RsU's). PRBAA is utilized to characterize the requests acquired from various nodes so as to furnish prompt reaction to crisis nodes with less time delay.

Index Terms: Elliptic Curve Encryption and Digital Signature (ECEDS), Preference Batch Authentication Algorithm (PRBAA), Sybil Attack, Vehicular Ad-Hoc Network (VANET).

I. INTRODUCTION

Vehicular Ad Hoc Network is profoundly about the fleet getting connected with one another by means of wireless networks. Some of the contemporary ways in which the unique connectivity takes place is by usage of the MANET and VANETs. While compared to the MANETs in the case of the VANETS there are more novel components that enable a robust network and correspondence.

It was demonstrated that vehicle-vehicle and vehicle-roadside interchanges designs will coincide in VANETs to give road security, route, and other road-side administrations [1]. VANET is a part of Intelligent Transportation Systems (ITS) structure. In VANET, communications are reassigned among nodes and additionally Road-side Units (RsU's).

Revised Manuscript Received on 30 January 2019.
***** Correspondence Author

Dr.K.Selvakumar*, Associate Professor, Department of Information Technology, Annamalai University, Chidambaram, Tamilnadu.

S.Naveen Kumar, Research Scholar, Department of Computer Science and Engineering, Annamalai University, Chidambaram, Tamilnadu.

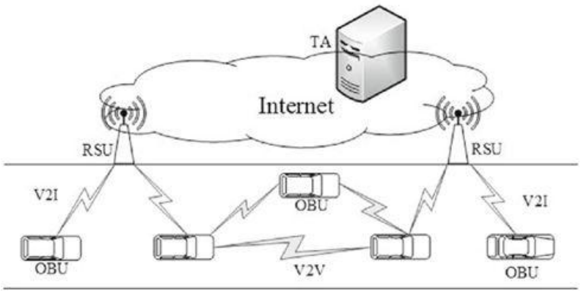


Fig.1 Architecture of VANET

The movement that involves the utilization of Secure Hash Algorithm (SHA-1) makes an excellent key for every message. The ECEDS at that point cause a multi key combine signature utilizing the SHA-1 key that fuses ECEDS domain specifications. Here we send the digital signature to the goal all alongside with the message [7]-[8]. The receivers verify the signature by utilizing SHA-1 key for the message, ECEDS and the multi key combine. In case the substantiation technique challenges single key combines, at that point the signature is checked; something else, the message was demolished on transmission. An Open-Key Infrastructure (OKI) is an arrangement of jobs, access, methods to form, convey, store, and repudiate approaches and open-key encryption. The basis of an OKI is to inspire the preserved electronic swap of information for an extension of network action, for a part, web based business, web managing an account and secret mail. Three distinct arrangements of messages can be used as an open-key cryptosystems are Encrypted message, Signed message, marked and scrambled message. Testaments commonly consolidate the owner's open-key, the lapse date of the authentication, the owner's name and alternative information about the open-key owner. False data revealed by a single malicious node may not be adequately persuasive. Applications may require a few nodes to strengthen specific data, previously tolerating it as truth. However, a significant problem issue emerges when a pernicious node can imagine as different nodes called a Sybil attack [12]-[14], and reasonably reinforce false information. On the off chance that favorable elements can't perceive a Sybil attack, they will trust the false data, and base their choices on it. Subsequently, tending to this issue is vital to useful vehicular system frameworks.

II. RELATED WORK

Around there, few past and improvements of SHA-1 and ECEDS are explained in [10], [11]. This section explores the previous work done on Sybil attack and their detection approaches in VANET. Malignant nodes can unfavorably affect this procedure by purposefully deliberately meddling in the middle of the packet exchange amid the nodes.

In this paper, we endeavored to protect against the Sybil attack with just help of Roadside Unit (RsU's). At whatever point a node passes the RsU's it acquires a timestamp. It is troublesome for multi nodes to acquire the equivalent timestamp while crossing various RSU's. Because of giving different timestamps it is unreliable for any attack. At the point when a node asks for different timestamps from a solitary RsU's, it implies quite possibly the node may go about as a Sybil attacker. The refreshing of timestamps is likewise known; rather than keeping the two timestamps in a message, another amassed timestamp has been made; it contains both the present and past timestamps. [16]

Secure group confirmation [17] [18] is completed to keep away from the invalid or false message from the unauthenticated or even validated nodes. By maintaining a strategic distance these false messages, road accidents and traffic jams can be counteracted to continue with the protected and safe shipment. A digital signature is utilized to guarantee the character verification and message integrity. A node signs the message with digital signature and then delivers it to the RsU's for confirmation. Proposed framework presents an algorithm to distinguish the SAISVs [19] [20] in VANET's. Also contains few Delivered Control Units (DCU's) in a VANET framework. In addition, these legitimate nodes can assemble and records the signature vectors from various DCU's in their development. Conversely, Sybil nodes have the similar areas and movement directions constantly. In every minute the signatures can give approved with timestamp. Every node can autonomously identify Sybil attack by contrasting the distinctions of adjacent nodes digital signature vectors; this algorithm is increasingly achievable even fewer framework assets. Here we present another sort of Sybil detection approach, in light of gotten signal quality varieties, enabling a node to check the validness of another transmitting node, as indicated by their restrictions. This paper gives Sybil attack discovery [21] approach dependent on gotten signal strength varieties. This methodology empowers a node to affirm the validness of nodes with which it is transmitting, by methods for two integral strategies, the check of their geological constrained and the assessment of their perceive capacity degree.

III. SECURITY IMPLEMENTATION

The fundamental work utilized to actualize the undertaking is that to give ECEDS. The ECEDS signature conspires are utilized by two components: an endorser A, and a verifier B. The endorser A signs the message N and conveys it to the verifier B. Here B will get the message N and affirm it. Without a doubt, any substance can check the signature on the off chance that it has A's open key. In some cases outsider can be included to check the signature of the message.

Element A should utilize the key arrangement method to set up a key combine. Element Y ought to have capacity to acquire the open key of A's. And A will utilize the key match so as to control the signing activity while B utilizes the open key required to control the confirmation step. At the point when 'A' needs communicate something specific N, it should sign the message utilizing its key matches and produce a signature R. Element A makes a message utilizing N and R, and send it to B. At the point when B gets the message, it applies the checking task utilizing A's open key so as to confirm the message validness. If the output of the confirming task is legitimate, then B will realize that the message N is real. At the end of the day, it originated from the endorser A.

A. ECEDS Area Parameters

ECEDS calculation needs that the private, and open keys utilized for digital signature creation and check be created as for a lot of area parameters. The area parameters are equivalent to a gathering of clients and might be open. Area parameters still remain made do with an all-encompassing time span. [5] - [9] The ECEDS area parameters are:

- *e (or) f*, are proportions of the essential field,
- *i*,j are the elliptic curve parameter may utilized to characterize the condition of the curve,
- $F = (Fa, Fb)$, in elliptic curve a point is known as a base point,
- *m*, requests the base point *F*,
- *l*, the elliptic curve separated by the order *m*, and is known as the cofactor.

B. ECEDS Private /Open Key

ECEDS key match comprises of private key *p*, and open key *O*. Every key match is related with an explicit arrangement of area limits. The private key *p*, open key *O*, and the area limits are mathematically identified with each other by means of the connection $O = pF$, where pF is the whole of p duplicates of the base point F. It is otherwise called elliptic curve scalar multiply of F by p. The private key *p* is utilized for a constrained timeframe (i.e. the crypto period). Then again, the open key *O* is utilized by the digital signature which is produced by the related private key is still being used because the digital signature needs to be confirmed. [5] - [9].

They doesn't utilized for different purposes (e.g. key establishment).

C. ECEDS Key Generation

All together for a substance to produce the key combine, it must ensure that the area parameters are substantial. Every key match is related with an explicit arrangement of domain parameters [5] - [9].

Producing the key combine is done as follows:

i) Select an irregular whole number p in the interim (1, *m*-1).

ii) Figure $O = pF$.

The outcomes are *p* and O, where p is the private key, and *O* (*Oa*, O*b*) is the open key.

D. ECEDS Signature Creation

A substance can sign a message *n* utilizing the key combination and the area limits. The result from the signing activity is a signature and is characterized by (u, *v*) [5]-[9]. The substance may follow to signs a message are:

i) Select a whole number *t*, where $1 \leq t \leq m$-1.

ii) Register *tO*= (*a1*, *b1*).

iii) Register *u* = *a1* [mod *m*]. On the off chance that u = 0, go to stage 1.

iv) Register *t*-1 [mod *m*].

Note: *t*-1 (mod *m*) is registered utilizing the inverse theory in Appendix C.

v) Register SHA-1(*n*), and change this string to a whole number S(*n*).

vi) Register *v* = *t*-1 (S(*n*) + *pu*) [mod *m*]. On the off chance that *v* = 0, go to stage 1.

(*u*, *v*) is the signature message.

E. ECEDS Concept Signature Authentication

To check a signature (*u*, *v*) on a message *n*, the recipient gets a duplicate of the sender's area limits, and its open key *O* [5] - [9]. It contains:

i) Check u, v are whole numbers, and in the interim (1, *m*-1).

ii) Process SHA-1(*n*), and changes this string into a whole number S(*n*).

iii) Process *z* = *v*-1 [mod *m*].

Note: *v*-1 [mod *m*] is processed utilizing the inverse theory in Appendix C.

iv) Process if *u1* = H(*m*)*w* [mod *n*], and *u2* = *rw*[mod *n*].

v) Process *A* = (*a1*, *b1*) = *d1F* + *d2O*.

vi)On the off chance that *A* = 0, dismiss the signature. Something else, process *g* = *a1*[mod m].

vii) Acknowledge the signature if *g* = *u*.

m is the signature to the message, checked when *g* = *u*.

IV. ATTACKS IN VANET

VANET is by and large progressively upheld for traffic control, accident avoidance, executives of parking areas and open regions. In VANET's, the different noteworthy worries are protection and security. Deplorably, in VANET's, most security protecting plans are powerless against Sybil attack.

A. Sybil Attack

A Sybil Attack is caused in VANET when a malicious node or RsU can obtain numerous characters. A Sybil attacker sends various messages with a particular false personality to different nodes in line. This makes a deception (or) confusion to other nodes in the similar path. It contains different sorts of nodes [13]-[16].

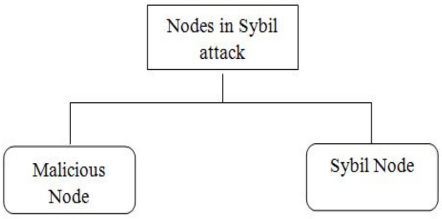


Fig.2 Nodes participates in Sybil Attack

(*a)* Pernicious node/ Sybil attacker: The node which spoofs the personalities of different nodes.

(b)Sybil node: The new characters made by the pernicious node to attack are known as Sybil nodes.

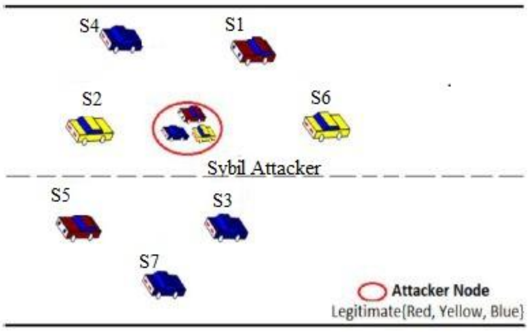


Fig.3 Sybil attack in VANET

In Fig.3, demonstrates the regular Sybil attack in VANET situation. Sybil attack is spoofing the personalities of S1, S2, and S3. The effect of Sybil attack gets severe serious when all characters made by attacker take an interest at the same time in the system. Sybil attack is grouped in two classes. The two are clarified below:

Step 1: The Sybil attacker makes the characters of the really current nodes in the system. Let W be the arrangement of all nodes in VANET, Y be the arrangement of all Sybil nodes. For this situation $(Y \subseteq W)$ (1)

Step 2: The Sybil attacker makes the characters from outside the system. For this situation $(Y \not\subset W)$ (2)

The Sybil attack makes diverse identities appropriate on time since each node is confirmed correspondingly with its open key.

In this attack, attacker makes diverse identities to reestablishing distinctive focuses. This attack is intense attack in which a node can asserted at better places with a few fake characters in the meantime and making enormous security hazards in the framework. A Sybil attack is unsafe for framework topologies and associations and in addition framework transmission capacity utilization. In this Fig.3 an attacker S1 exchanges numerous messages with various characters to alternate nodes. Along these lines, different nodes see that there is as of now a massive traffic. [16]

V. PROPOSED MODEL

We acquainted the proposed model with counteracting Sybil attack utilizing attack avoidance calculation and furthermore moreover introduced the Preference Batch Authentication Algorithm (PRBAA) to give a prompt reaction to the crisis. When an RsU gets numerous requests from various nodes at an equivalent time, the time deferral can strike process all of them and it doesn't give a speedy reaction to crisis nodes like rescue vehicle, fire, and police.

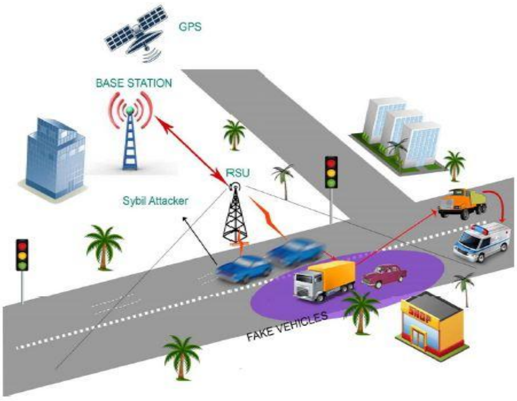


Fig.4 The Sybil attack prevention model

A. Proposed Sybil Attack Prevention Mechanism

In wellbeing functions, nodes can make an impression on neighbor nodes; nodes require a timestamp. It needs to connect timestamps in each message. At the point if a node acquires different timestamps from a solitary RsU's then it might go about as an attacker and deliver a Sybil message to different nodes so as to go astray (or) back them off. While accepting numerous messages from various nodes, authentic nodes pick that some mishap or traffic has occurred and taken another course (or) diminishes its speed. It isn't essential to give a timestamp to a solitary node inside a brief timeframe by RsU. Our attack counteractive action calculation restrains the giving of relentless timestamps [22] to the specific node inside a brief period between times. A node in the timestamps first time decides to set the timer after it gives by the RsU. Before the clock lapses a node again sends an interest for timestamp which infers perhaps the node might be an attacker at that point RsU denies give timestamp and disposes of the interest and thereafter tracks the node discover whether the node is an attacker (or) a real node.

a) Algorithm

```
i) Start
ii) Node send_reqs to RsU
iii) RsU gives TSP to nodes
iv) Later ACKM, RsU decides clock TI
v) In the event that (send_reqs<=TI)
vi) Return "quit giving TSP to nodes"
vii) Return "Track the node data"
viii) Else
ix) Return "give TSP"
x) Stop
```

The algorithm explains that the proposed calculation of Sybil attack prevention component.

B. Proposed Ideal of Preference Batch Authentication Algorithm

In a similar time single RsU can receives demands from different nodes. By and large, RsU performs activity on those got demand by utilizing batch authentication calculation and give required administrations to the nodes.

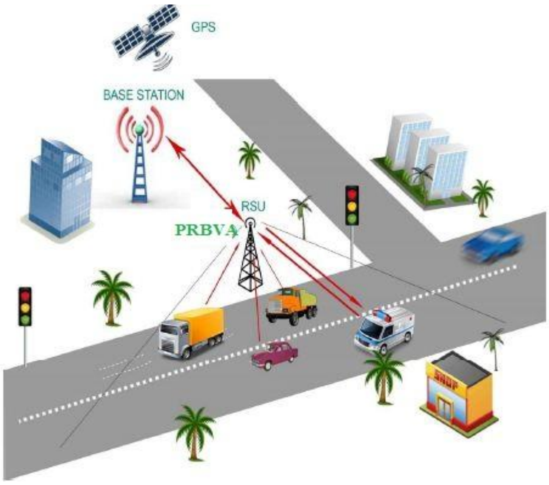


Fig.5 model of proposed PRBAA

The above Fig.5 demonstrates the proposed model of PRBAA Mechanism.

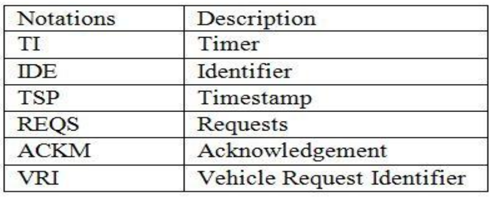
In any case, it doesn't appoint any need and give reaction to the demand from crisis nodes [15]-[16]. It is vital to give quick administrations to crisis nodes. The proposed model of Preference Batch Authentication Algorithm (PRBAA) is introduced in every RsU's. If an RsU gets numerous requests in the meantime, PRBAA forms these requests so as to recognize any demand got from crisis nodes. In the event that RsU's demands from crisis nodes our mechanism PRBAA promptly forms these requests and sends important administrations to that node immediately.

a) Algorithm

```
i) Start
ii) RsU got PB= {reqs1, reqs2… reqsm}
iii) N1,….Nm=reqs1,reqs2,…reqsm
iv) N[m]=reqs[m]
v) For (j=0;j<m;j++)
vi) Order the requests
vii) In the event that (reqs[ide]==vri1)
viii) Return "Ambulances"
ix) Return "give administration to the demand"
x) Else if (reqs[ide]==vri2)
xi) Return "fire and Police Nodes"
xii) Return "give administration to the demand"
xiii) Else
xiv) Return "General Nodes"
xv) Return "security and non wellbeing administrations"
xvi) End if
xvii) Stop
```

The code clarifies explains that proposed mechanism of preference batch authentication calculation.

Table 1: Notations



Notations	Description
TI	Timer
IDE	Identifier
TSP	Timestamp
REQS	Requests
ACKM	Acknowledgement
VRI	Vehicle Request Identifier

VI. NETWORK SIMULATION

Here we assess the execution of our proposed protocol in significant viewpoints. In this work, we proposed actualized and incorporated algorithm is ECEDS. At that point information was produced, which enabled us to make a standard algorithm execution on a VANET and perusing the outcome next. Here we can see that, in this underlying situation, nodes are found in an area with a separation littler than 100m. Here the nodes are inner the system range and there was no package was disposing of. Utilizing a situation of 10 nodes, where node "0" delivers a communicated message to alternate nodes from the system. Consequently we feature the productivity of ECEDS, as per what has been tried (tested) by different works already made reference to, however in various contexts of VANET networks

A. Packet Delivery Ratio (PDR)

This is characterized as the total quantity of packets effectively deposited to the total sent packets. PDR describe as the quantity of packets is deliver from origin to terminal if the proportion of the network is expanded in any strategy that implies by utilizing this procedure network assistance improves. The formula for PDR is:

PDR = (RCV/SND)*100

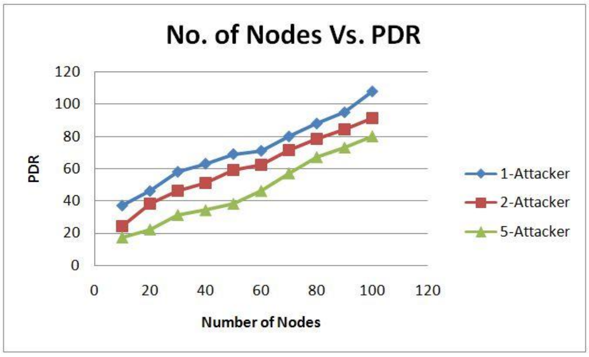


Fig.6 PDR w.r.t Nodes

B. Throughput

Throughput is a part of how many units of information a system may processed in the given time. Throughput characterizes as the measure of information come truly from a station to another station. Bits are exchanged from starting with one place then onto another place in every second. On the off chance that the throughput is high then data transfer capacity. Usage is better beneath us notice the formula of throughput as:

Throughput = bitspersecond

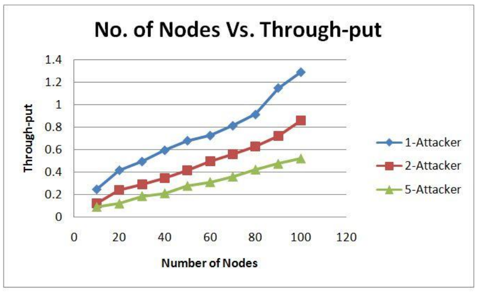


Fig.7: Through-put w.r.t Nodes

C. End to end delay

It is imperative to find the bang of encryption overhead on the end to end delay with expanding measure of nodes and speeds.

$$d_{end\text{-}end} = N[d_{trans} + d_{proc} + d_{proc} + d_{queue}]$$

Where

d_{trans} = transmission delay

d_{proc} = propogation delay

d_{proc} = processing delay

d_{queue} = Queuing delay

N = number of links (Number of routers -1)

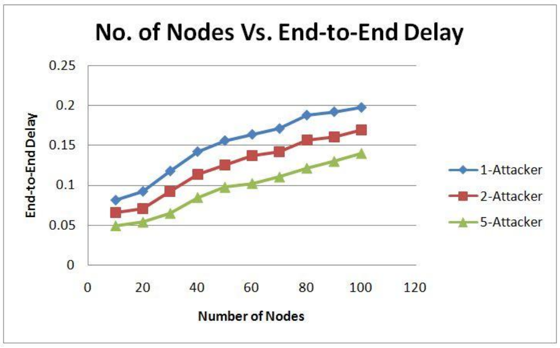


Fig.8: Packet over Head w.r.t Nodes

D. Packet over Head

The time it proceeds to broadcast the information on a packet-switched framework. Every packet needs additional bytes of format data which is stored in the packet header, when mixed with the assembly and disassembly of packets, decreases the overall transmission speed of the crude information. Here the graph shows a packet over head diagram between the current and proposed approach. The proposed methodology is longer in the overhead protocol than the base methodology.

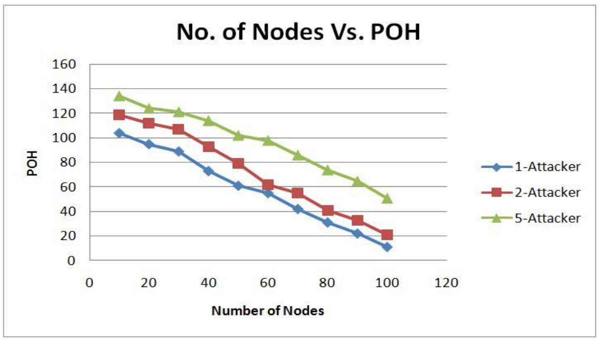


Fig.9: Packet over Head w.r.t Nodes

VII. CONCLUSION

The current research challenges of VANET's broadcasting protocols are focused on issues such as ECEDS. Security is a major challenge in implementation of VANET's. In this survey article, we have presented security measures to be taken before implementing a VANET. The major issues in VANET's are privacy and authentication. The security examination of our proposed convention shows the flexibility across different security risk. Our proposed framework PRBAA algorithm is utilized process various demand at a solitary time and furthermore to give quick reaction to the demand from crisis nodes. By attack counteractive action component the Sybil attack itself starts the timestamps.

In future, we will counteract attack, without confining the arrangement of timestamps to nodes and limit the calculation work of algorithm. As we increment number of nodes it might outcome in more defer which builds the bottlenecks in system correspondence.

REFERENCES

1. Pathan, Al-Sakib Khan , "Security of Self- Organizing Networks: MANET, WSN, WMN, VANET ", CRC press, 2011.
2. Ram Shringar Raw, Manish Kumar, Nanhay Singh "security challenges, issues and their solutions for vanet"sept 2013.
3. priyanka sirola, amit joshi, kamlesh C. Purohit "An Analytical Study of Routing Attacks inVehicular Ad-hoc Networks (vanets)"July 2014.
4. ANSI X9.62-2005, 2005. "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)". American National Standards Institute, November 2005.
5. FIPS 186-3, 2009. "Digital Signature Standard (DSS)". Federal Information Standards Processing Publication 186-3, National Institute of Standards and Technology, June 2009.
6. M. Raya and J. Hubaux, ''The security of vehicular ad hoc networks'', in Proc. 3rd ACM Workshop Secur. Ad Hoc Sensor Netw., 2005, pp. 11–21.
7. SEC1 Standards for Efficient Cryptography Group, SEC 1: Elliptic Curve Cryptography, Version 2.0, 2009.
8. FIPS 186-3, 2009. "Digital Signature Standard (DSS)". Federal Information Standards Processing Publication 186-3, National Institute of Standards and Technology, June 2009.
9. Sabahi.F, "The Security of Vehicular Adhoc Networks", In Computational Intelligence, Communication Systems and Networks (CICSyN), 2011 Third International Conference on 2011 Jul 26 (pp. 338-342). IEEE.
10. Manvi, S.S.; Kakkasageri, M.S.; Adiga, D.G, "Message Authentication in Vehicular Ad Hoc Networks: ECDSA Based Approach", *Future Computer and Communication, ICFCC 2009. International Conference on* , vol., no., April 2009, pp.16-20, 3-5.
11. "Public Key Cryptography for the Financial Services Industry: The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62-2005, American National Standards Institute, November 2005.
12. Jaydip kamani,Dhaval parikh "A Review on Sybil Attack Detection Techniques"Mar 2015.
13. Chaitanya Kumar Karn and Chandra Prakash Gupta, "A Survey on VANETs Security Attacks and Sybil Attack Detection", in International Journal of Sensors, Wireless Communications and Control, 2016, 6, 45-62.
14. Kafil P, Fathy M, Lighvan MZ. "Modeling Sybil attacker behavior in VANETs", Information Security and Cryptology (ISCISC), 2012 9th International ISC Conference on 2012 Sep 13 (pp. 162-168). IEEE.
15. Vinh Hoa LA, Ana Cavalli "security attacks and solutions in vehicular ad hoc networks: a survey"april 2014.
16. "Prevention of Sybil attack and priority batch verification in VANETs", by P. Vinoth kumar and M. Maheswari, ICICEs 2014.
17. Zhang Jianhong, Xu Min and Liu Liying, "On the Security of a secure Batch verification with Group Testing for VANET", International Journal of Networks, Vol.16, No.4, PP.313- 320,2014.
18. Jiun-Long Huang, Lo-Yao Yeh, and Hung-Yu Chien," ABAKA: An Anonymous Batch Authenticated and Key Agreement Scheme for Value-Added Services in Vehicular Ad Hoc Networks" IEEE Transaction On Vehicular Technology, VOL. 60, NO. 1, Janauary 2011.
19. Chen Chen, Weili Han and Xin Wang, "Sybil attack detection based on signature vectors in VANETs", Int. J. Critical Computer-Based Systems, Vol. 2, PP 455,2011.
20. Karamjeet Kaur , Sanjay Batish & Arvind Kakaria, "Survey of Various Approaches To Countermeasure Sybil Attack", International Journal of Computer Science and Informatics ISSN (PRINT): 2231 –5292, Vol-1, Iss-4.,2012.
21. Mohamed Salah Bouassida, Gilles Guette, Mohamed Shawky and Bertrand Ducourthial, "Sybil Node Detection Based on Received Signal Strength Variation" International Journal of Network Security, Vol.9, No.1, 2009.
22. Soyoung Park,Baber Aslam,DamlaTurgut,Cliff C. Zou, "Defense against Sybil attack in vehicular ad hoc network based on roadside unit", IEEE conference Paper ID 900042,2009.

AUTHORS PROFILE

Dr.K.Selvakumar obtained his Bachelor's Degree in Electronics and Communication Engineering in Kongu Engineering College, and the Master's Degree in Communication Systems from NIT Trichy, and Ph.D in Computer Science and Engineering from Annamalai University. He works as Associate Professor in Annamalai University. He has 29years of experience in teaching. His area of interest includes Cryptography and Wireless Network, Network Security, Mobile Computing.

S. Naveen Kumar obtained his Bachelor's Degree in Computer Science and Engineering in Annamalai University, and the Master's Degree in Computer Science and Engineering in S.V University, tirupati. He is currently working towards Ph.D degree at Annamalai University. His research interests include Wireless Networks, Vehicle Ad-Hoc Networks, and Network Security.