
Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issue 1, pp. 41–46, DOI 10.12694:/scpe.v21i1.1608

SECURED IDENTITY BASED CRYPTOSYSTEM APPROACH FOR INTELLIGENT ROUTING PROTOCOL IN VANET

A KARTHIKEYAN *, P G KUPPUSAMY† AND IRAJ S AMIRI* ‡

Abstract. Vehicular specially appointed systems named as Vehicular Ad-hoc NETwork (VANET) have been raising dependent on the condition of-art advancements in remote and system communication. The message confirmations among vehicles and infrastructure are fundamental for the VANET security. The genuine personality of vehicles ought not to be uncovered, yet which is just detectable by approved nodes. Existing arrangements either depend vigorously on a carefully designed hardware or cannot fulfill the security necessity. Secured Identity Based Cryptosystem Approach (SIDBC) for intelligent routing protocol is proposed for better results since implementing a secured network for traffic forecasting and efficient routing in dynamically changing environment. Polynomial key generation is utilized for generating identity based pseudonym keys for each and every node that comes under the system. This keying process protects the node from malignant node from passing false information. The assessment output demonstrates that the planned method is more effective than past schemes since it is free pairing and it fulfills security and protection prerequisites.

Key words: Data rate, Vehicular Ad hoc Networks, Trust Authority, Message Authentication, Polynomial Keys.

AMS subject classifications. 68M15

1. Introduction. VANET can be described in simple manner i.e. the vehicles that moves in the roadways are interconnected virtually by passing messages among them. It acts as a kind of Mobile Ad-hoc Networks (MANET) that comprises of mobile nodes and operates in a decentralized way. Infrastructure condition in which, moving devices can be in connection continuously. It is fundamentally formed by those elements that deal with the traffic or offer an outside administration. On one hand, producers are once in a while considered inside the VANET model. A few unique functions are rising in VANETs that incorporates well-being related applications to make more secured driving, portable business and other data benefits that will illuminate drivers about any kind regarding clog, driving perils, mishaps, roads turned traffic jams.

The paper organised is as follows section describes a formal introduction of VANET, section 2 depicts overview of VANET, section 3 describes the proposed security identity based algorithm, section 4 deals with the result analysis of the proposed and existing mechanism and section 5 provides the conclusion of this proposed methodology.

2. Related Works. IVC comes under the operating system of VANETs which turn out to be admired in current years [1]. The vehicles function here as mobile nodes and they are connected together wirelessly. The principle contrast is that versatile switches which manufacture the system are vehicles like cars or trucks. Many academic communities are working for enabling new applications with respect to VANETs [2, 3] for reducing road hazards. Significant role of the method is to enhance the road safety measures.

Several safeties related approaches have been undertaken in VANET environments to enable secure information transmission among vehicles. Identity aware system that has main impacts in reducing accidents and increasing traffic control services were discussed, here the information is shared among them in a timely manner. Public Key Algorithms (PKA) was proposed [4, 5, 6] for providing safety measurements during information

*Associate Professor, Department of Electronics and Communication Engineering, Vel Tech Multi Tech Dr.Rangarajan Dr.Sakunthala Engineering College, Avadi, Chennai, India. (a.karthik1982@gmail.com)

†Professor, Department of Electronics and Communication Engineering, Siddharth Institute of Engineering & Technology, Puttur, Andhra Pradesh, India, (kuppusamy.pg@sgiptr.com)

‡Computational Optics Research Group, Advanced Institute of Materials Science, Ton Duc Thang University, Ho Chi Minh City, Vietnam. Faculty of Applied Sciences, Ton Duc Thang University, Ho Chi Minh City, Vietnam. (irajsadeghamiri@tdtu.edu.vn)

exchange in Ad-hoc networks. Symmetric keys are generated by the system and master keys are loaded as per arbitrary distribution.

To protect the road environments from false information and privacy of the vehicles a provably secure batch-verification method was proposed. Privacy preserving mechanism [7, 8] for secured vehicular communication includes priori and posteriori counter measures for identifying the number of anonymous vehicles present in RSU. Based on threshold value the priori and posteriori messages can be set and the batch of messages can be verified in a single turn. Scalable Robust Authentication protocol for secured vehicular network was proposed [9], here the group signatures is employed for each RSU rather than centralized authority. RSU preserves and manages the on fly group communication to the uphold range. Anonymous messages passed by the vehicles can be instantaneously verified by the other vehicles that present in the same RSU. If received message resulted to be duplicate then the message originator identity is declared to every vehicle. Identity based security scheme was proposed to achieve privacy in information sharing with fundamental security needs like confidentiality, non-repudiation and authentication. Here privacy preserving defense mechanism [10] was proposed to identify misbehaving vehicles using network authorities. A pseudo-identity-based scheme [11] for conditional anonymity with integrity and authentication in a VANET was proposed and it provides conditional anonymity to guarantee the protection of an honest vehicle's real identity, unless malicious activities are detected. Certificates are not required in this mechanism since identity based cryptosystem is employed for authenticating the vehicles. Efficient Privacy-Preserving Data-Forwarding Scheme (EPPDFS) [12] was proposed to examine the security aspects in VANET and to increase the user privacy efficiency. Lite Certificate Authority (CA) based Public Key (PK) cryptosystem and route-generate encryption schemes are proposed in EPPDFS. Secure and efficient authentication scheme (SEAS) [13] with unsupervised anomaly detection. Here, certificateless authentication method is deployed for conditional privacy preserving, along with the Chinese remainder theorem for efficient group key distribution and dynamic updating [16]. A cryptographic primitive scheme [15] was proposed for public updating of reputation score based on the Boneh-Boyen-Shacham short group signature scheme. This allows private reputation score retrieval without a secure channel.

3. Proposed Algorithm. SIDBC technique for intelligent routing protocol is proposed; here each task is carried out by different agent allotted for the particular task. Then the agents are cooperatively interacted to form a reliable network structure. Road Side Units (RSU's) are placed in the infrastructure and On Board Units (OBU's) are placed in the vehicles and the communication takes place with the help of this devices. Regional Transport Authority provides security keys for vehicles and RSU's. Routing the packets securely and efficiently with the help of cooperative multi-agent mechanism greatly improves the network throughput [15].

3.1. IDC Authentication Offer. Initially each node registers to the Trust Authority (TA) and security analysis is made for every node that participating in the network. Identity based Cryptosystem (IDC) is used to provide secured environment during data transmission among nodes. IDC allows PK to be derived from its communal identity. Regional Transport Authority (RTA) establishes trust relationship between the nodes using pair-wise keys. RTA generates public/private keys for each and every node that entered into the network. Each RSU is connected to RTA and pre-established keys are generated for trusted region. RSU generates pseudonym for every node that entered into the region using Polynomial Key Generation (PKG). This pseudonym is used to identify the malicious vehicles that access the lane for privacy-conserving authentication and secure communication.

Trust Authority creates pseudonym for every node as given below:

$$T_A = PK(id)_n \, \|T_p\| \, C_n \tag{3.1}$$

where,

$T_P \rightarrow$ Present Time
$PK(id)_n \rightarrow$ PK identity of node N
$C_n \rightarrow$Code name of every node

The source vehicle broadcast the route request message to their neighbor vehicle up to the communication range or the bounded cluster region. Control Request message consist of this parameters such as

$$CR = \langle ID_s, T, HD, I_N, Nf, SIG(Id_d, T) \rangle \tag{3.2}$$

where,

$Id_s \rightarrow$ Src node ID
$T \rightarrow$ Timestamp
$HD \rightarrow$ Node's codename
$I_N \rightarrow$ Invite the node
$Nf \rightarrow$ Node's Freshness
$SIG(Id_d, T) \rightarrow$ Signature (key) for sink node with Timestamp.

CH or the vehicle node that present in the cluster region accepts this control message during the present time gap. Later the nodes launch reply message back to the source via intermediate vehicles through SA. Control Reply message contains,

$$C_{RP} \leftarrow ID_d, P_s, T, connect, SIG(P_s, T) \tag{3.3}$$

where,

$ID_d \rightarrow$ Destination node ID
$P_s \rightarrow$ Pseudonym generation
$connect \rightarrow$ Connect request message
$SIG(P_s, T) \rightarrow$ Signature generated for pseudonym node with timestamp.

The source receive the control reply message from these nodes, the source confirms the signed key and acknowledge it, if the information is verified. In case the false or malicious vehicle transmits a phony validation message, the TA can open the represented signed key to stamp out the genuine personality of the vehicle. If TA distinguishes any malicious vehicle then it passes a warning message to all the vehicles surrounded by it.

3.2. Key Generation Process. When the authenticity of the hub is demonstrated with their sign confirmation, then the declarations are affirmed from CA. In the event that another hub is participated in the system and set as a switch, at that point the hub requires its substantial character. Without authentication the hub cant process the data further. Two connection keys ate gotten from the pr-evaluated values (eg., Lk and Qv) and it is produced from the Node ID. When the authenticity of the node is demonstrated (Lk, Qv and Sidi) at that point the two hubs can impart. In key concern stage, nodes are approved for keeping it from trickery and pantomime assaults. Here the node A make sense of the node B open key utilizing its certU and CA key's QCA. The private key 'KAB' calculation at together closures is by all accounts indistinguishable just when the endorsements are designated by the legitimate CA. The irregular key generator produces the mystery key Mk for the message encryption process. Each message comprises of basic verification of message authenticated code key 'K' and this key shield the message from the change by the malignant nodes.

3.3. Data Processing Process. Base station initiates authentication process once the request message received; the node is verified for legal access by using sign authentication system. Once the signing process finished the certificate is provided for the legitimate nodes also the communication encoding process gets done. Source node sends the encrypted message using hash algorithm and the encryption process commonly includes general authentication key. Then the EMK is sent to the destination with the valid token $CA, Sidi(K)$ added in the header field of the encrypted message.

$$EM_k = M \parallel L_k, Q_v, Sidi, K \tag{3.4}$$

4. Simulation Result Analysis. The results demonstrate various types of reproduction parameters utilized in the proposed secured information of convention reenactment. Proposed scheme is analyzed using the parameters like Delivery Rates of data packet (PDR), Average delay and Throughput.

- Delivery Rate of data packet

Delivery Rate of data packets can be computed by taking the ratio between the sum of number of packets that reached over the sink node and the sum of packets sent by the source vehicle. It is obtained from the equation (4.1) below.

$$PDR = \frac{\sum PktsDelivered}{Time} \tag{4.1}$$

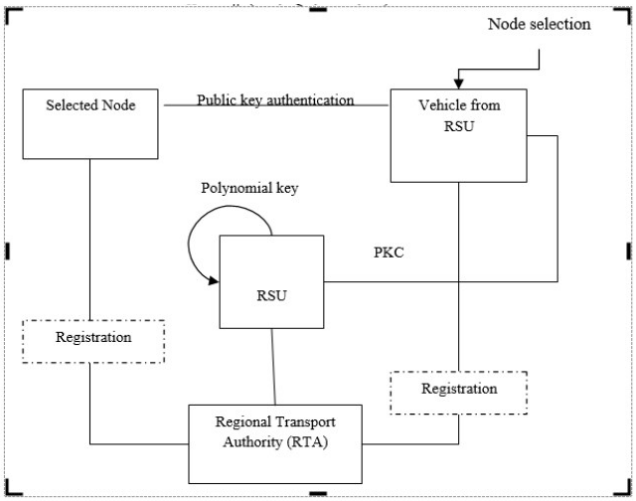

FIG. 3.1. *IDC Authentication Offer*

TABLE 3.1
Algorithm 1

Set N number of nodes
Registered with BS
Create Sign for each registered node N_i using PKG
Set source node 'A' and sink node 'B'
Check NI_d for node verification
Set pseudonym key ¥n
If NI_d(key) matches then provide nodes with certificate 'CertA'
Do node validation $L_k, Q_v, Sidi$
Create Private Key for legitimate nodes $L_k, Q_v, Sidi, K$
Apply keying function $M \parallel L_k, Q_v, Sidi, K$
Send secured data from A to B

E_{PDR} - PDR referred for existing protocol
P_{PDR} - PDR referred for proposed protocol

Here *PktsDelivered* is the number of packets arrived to destination and *PktsSent* is the number of packets sent by the vehicle. The proposed method SIDBC have better delivery rates of packets at the destination compared to the existing system SEAS and it is shown in figure 4.1.

- *Throughput*
  It is described with their rate of effective transmission of data.

$$Throughput = (\frac{PacketsReceived \cdot 8}{Delay\ in\ ms}) \text{ kbps} \tag{4.2}$$

  The throughput of the proposed SIDBC gives better result compared to the conventional SEAS method. When delivery rates increases then throughput also increases gradually (figure 4.2).
- *Delay*
  It is characterized as the time contrast between the present data packets received and the received time of past packets.

$$Delay = \frac{\sum_0^n Pkt\ recvd\ Time\ - Pkt\ send\ Time}{n} \tag{4.3}$$

  From the figure 4.3, it is clearly shows that the average delay of the proposed SIDBC scheme has consumed lesser time delay for transferring the packets compared to the SEAS (E-Dly.tr) protocol.

FIG. 4.1. *Delivery Rates of packet*

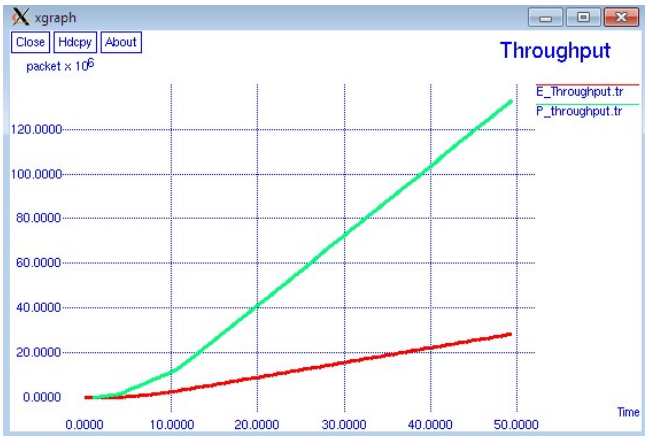

FIG. 4.2. *Throughput*

FIG. 4.3. *Delay*

5. Conclusion. A Secured Identity Based Cryptosystem Approach for intelligent routing protocol is proposed for better results since implementing a secured network for traffic forecasting and efficient routing in dynamically changing environment is a challenging task. So as to ensure that it can fulfill message confirmation necessity, existential enforceability of fundamental signed key against adaptively selected message attack. Polynomial key generation is utilized for generating identity based polynomial keys for each and every node comes under the network. The evaluation results show better efficiency rate compared to previous methods as shown in the result analysis f throughput and delivery rates.

REFERENCES

[1] L. L.ayuan and L.Chunlin, *A Qos multicast routing protocol for clustering mobile ad hoc networks*. Computer Communications, 307(2007), pp, 1641-1654.

[2] X. Yang,J. Liu, F.Zhao, and N. Vaidya," *A vehicle- to-vehicle communication protocol for cooperative collision warning*," Proc.Int.Conf.MobiQuitous,2004,114-123.

[3] A. Nandan, S.Dass,G.Pau, M.Y.Sanadidi, M. Gerla," *Car Torrent: A Swarming Protocol for vehicular networks*", IEEE INFOCOM, Miami, Florida, March 2005.

[4] J.Zhao and G. Cao, " *VADD: Vehicle-assisted data delivery in vehicular ad hoc networks*," IEEE Transaction Vehicular Technology, Vol.57, N0.3,pp. 1910-1922, May 2008.

[5] R.Ahlswede, N. Cai, S.Y.R. Li, and R.W. Yeung, "*Network Information flow*, " IEEE Transactions on Information Theory, vol.46, no. 4, pp.1204-1216,2000.

[6] M. Sardari, F. Hendessi, and F.Fekri, " *DDRC: Data Dissemination in Vehicular Networks Using Rate less Code*s", presented at J.Inf.Sci.Eng.,2010,pp.867-881

[7] Xiumin Wang, Jianping Wang and V. Lee, " *Data Dissemination in Wireless Sensor Networks with Network Coding*," EURASIP Journal on Wireless Communications and networking, vol. 2010, Article ID 465915, 14 pagess, 2010.doi: 10.1155/2010/465915

[8] Halford, Thomas R., Thomas A. Courtade, Keith M. Chugg, Xiaochen Li, and Gautam Thatte. "*Energy-efficient group key agreement for wireless networks*." IEEE Transactions on Wireless Communications 14, no. 10 (2015): 5552-5564.

[9] Zhang, Lei, Qianhong Wu, Agusti Solanas, and Josep Domingo-Ferrer. "*A scalable robust authentication protocol for secure vehicular communications*." IEEE Transactions on vehicular Technology 59, no. 4 (2010): 1606-1617.

[10] Sun, Jinyuan, Chi Zhang, Yanchao Zhang, and Yuguang Fang. "*An identity-based security system for user privacy in vehicular ad hoc networks*." IEEE Transactions on Parallel and Distributed Systems 21, no. 9 (2010): 1227-1239.

[11] Dong, Xiaolei, Lifei Wei, Haojin Zhu, Zhenfu Cao, and Licheng Wang. "*EP^{2}DF: An Efficient Privacy-Preserving Data-Forwarding Scheme for Service-Oriented Vehicular Ad Hoc Networks*." IEEE Transactions on Vehicular Technology 60, no. 2 (2011): 580-591.

[12] Alazzawi, Murtadha A., Hongwei Lu, Ali A. Yassin, and Kai Chen. "*Efficient Conditional Anonymity with Message Integrity and Authentication in a Vehicular Ad-Hoc Networ*k." IEEE Access (2019).

[13] Tan, Haowen, Ziyuan Gui, and Ilyong Chung. "*A Secure and Efficient Certificateless Authentication Scheme with Unsupervised Anomaly Detection in VANETs*." IEEE Access 6 (2018): 74260-74276.

[14] Chen, Liqun, Qin Li, Keith M. Martin, and Siaw-Lynn Ng. "*Private reputation retrieval in public–a privacy-aware announcement scheme for VANETs*." IET Information Security 11, no. 4 (2016): 204-210.

[15] Jayarajan, P., Kanagachidambaresan, G.R., Sundararajan, T.V.P. et al. J Supercomput (2018). http://sci-hub.tw/10.1007/s11227-018-2582-4

[16] E. Kayalvizhi, A. Karthikeyan, J. Arunarasi, "*An Optimal Energy Management System for Electric Vehicles using Firefly Optimization Algorithm based Dynamic EDF Scheduling*", International Journal of Engineering and Technology, vol. 7, no. 4, Aug-Sep 2015.

Edited by: Swaminathan JN
Received: Sep 24, 2019
Accepted: Dec 16, 2019