Dharanyadevi et al. 2016. *Int. J. Vehicle Structures & Systems*, 8(2), 82-85
ISSN: 0975-3060 (Print), 0975-3540 (Online)
doi: 10.4273/ijvss.8.2.04

International Journal of Vehicle Structures & Systems
Available online at www.maftree.org/eja

Technical Note on Secure Service Access in VANET using PBKDF Algorithm

P. Dharanyadevi[a], T. Divyasree[b, c], S.P. Sharmila[b, d] and K. Venkatalakshmi[e]

[a]*Information and Communication Engg., Anna University, Chennai, India*
Email: dharanyadevi@gmail.com
[b]*Dept. Information Technology, Madras Institute of Technology, Anna University, Chennai, India*
[c]*Email: divyasree175@gmail.com*
[d]*Email: prabhakarsharmila@gmail.com*
[e]*Electronics and Communication Engg., Anna University, Tindivanam, India*
Email: venkata_krish@yahoo.com

ABSTRACT:

Vehicular networks and their applications have gained great attention to the research community and vehicle industry in past few years. The applications in Vehicular Ad-hoc Networks (VANETs) are growing rapidly. The two main application classes have lately gained popularity such as secured and non secured applications. In this paper, we focus on security in VANETs using Packet Bit Key Data Function (PBKDF) Algorithm. The performance of proposed algorithm is assessed using Simulation of Urban Mobility (SUMO) coupled with V2X simulation runtime infrastructure.

KEYWORDS:

Vehicular Ad-hoc Networks; Security; Service access; Performance

CITATION:

P. Dharanyadevi, T. Divyasree, S.P. Sharmila and K. Venkatalakshmi. 2016. Technical Note on Secure Service Access in VANET using PBKDF Algorithm, *Int. J. Vehicle Structures & Systems*, 8(2), 82-85. doi:10.4273/ijvss.8.2.04

1. Introduction

The applications related to intelligent transportation systems which were potentially increasing in number have attracted by the researchers in the domain of networking in Vehicular Ad-hoc NETworks (VANETs) [1-3]. VANETs are also known under a number of different terms such as inter-vehicle communication (IVC), Dedicated Short Range Communication (DSRC) or Wireless Access in Vehicular Environment (WAVE). The goal of most of these projects is to create new network algorithms or modify the existing for use in a vehicular environment. The most vital challenges of wireless communications deal with information security among communicating parties, especially in the case of VANET due to the dynamic behaviour of vehicles. VANET also has unique features that distinguish its characteristics from other mobile ad hoc networks. The most important characteristics are mobility, distributed communication, limitations of road pattern, and no network size limitations. All these distinctiveness made VANETs environment an exigent for developing a secured milieu.

A detailed description of different threats of attacks can be found in [4-7]. A perspective on attack modelling in some vehicular scenarios is presented in [8]. In this research, secure service access for location based service discovery in VANET is focussed. In a vehicle to vehicle communication, major concern is the addition of false information by manipulating position, speed parameters or even identities. Moreover, as described in [9] denial of service attacks can be caused by jamming the link layer radio channel forwarding capacity at the network layer. As a result of the network attacks impose the risks, various proposal types for authenticating and securing data have been proposed in providing the reliable communications in VANETs [10-11]. Kaouther et al have proposed efficient and scalable LocVSDPs for vehicular networks. The proposed protocols have vehicles provided with an efficient mechanism to locate service providers and how to reach them (routing) simultaneously [12]. As depicted in Table 1, the proposed system focuses on the secured service access. This work describes a secure service architecture based on the key activation function which provides time based session parameters for on-demand services intended for vehicular to infrastructure communications.

Table 1: Comparison between existing and proposed system

Existing system	Proposed system
Mainly focus on service discovery	Mainly focus on security in service discovery process
No security algorithm is used	Uses secure PBKDF Algorithm
Malicious attackers may retrieve the services during reply propagation phase	No malicious attackers can access services

2. Packet Bit Key Data Function (PBKDF) algorithm

A secure access mechanism is needed to access the services securely in an effective manner. When a driver or passenger is in need of accessing a service which is to be very confidential, the secure access mechanism should perform the process of secure service access without any interference of vehicular attacks. Fig. 1 illustrates the network architecture diagram for the

proposed PBKDF, which describes the flow of request and response to secure service access in the VANET. In this system model, Road Side Units (RSUs), Client Vehicles (CVs) and Intermediate server (IS) are considered. RSUs have routing capabilities, and are fixed or have low mobility. They are clustered into one or more RRs. RRs in one cluster are connected to each other within the range and form an IEEE 802.11 based wireless roadside cluster (RCi) in a cluster i. CVs are characterized by their high mobility and amplified density. In common, vehicles have incorporated devices and may carry zero or one wireless interface. Vehicles without a wireless interface will not use the service discovery protocol. Thus, they will not impinge on the mechanism. Vehicles equipped with the wireless interface use the interface for ad-hoc communication with each other and with the RRs. The IEEE 802.11 is used for the wireless communication between vehicles and RRs. The wireless connection between two vehicles could be performed directly or through RRs in a cluster. IS plays a vital role in the proposed system which means providing security. Encryption of data is processed by this element.

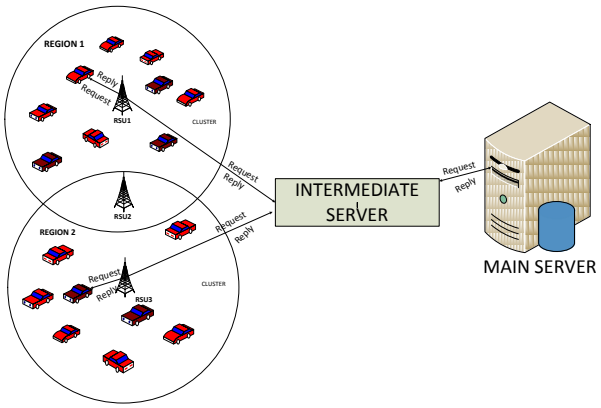

Fig. 1: Network architecture for PBKDF

The proposed system focuses on the security measures in VANETs. Security provides for service access is enhanced by processing the PBKDF algorithm in intermediate server. In AODV, the network is silent until a connection is provided. At that point need for broadcasting the connection to the node is necessary to request for a link. Other AODV vehicles forward this message, and document the node that they listen to it from, creating a bang of momentary routes back to the needy node. When a relay node has a pre-defined path and a message to the desired node, it sends a message backwards through a temporary route to the requesting node. The requested node then begins using the route that has the least number of hops all the way through other nodes. Vacant entries in the routing tables are recycled after a time. Table 2 describes the technical terms which were used to enhance the encryption technique in the proposed algorithm. The following paragraphs detail the phases in the proposed system.

- Broadcasting the MsgID: Client Vehicle (CV) in VANET when comes under Dedicated Short Range Communication (DSRC) will broadcast the MsgID to their neighbour nodes and their corresponding RR. This phase helps all the CV to know the status of other CV for communication, for exchange of messages, service access and so on.
- Service Requisition Phase: A CV (driver or passenger) generates a request for a location based service. This request is forwarded to the corresponding RSU. When the service request is to be transmitted, processing ID is generated. This ID is piggybacked to all the nodes by which the request is propagated to the Main Server. Before generating the service response message, it will validate the MsgID and Processing ID to avoid service attacks.
- Service Encryption Phase: After validating the MsgID and the processID of the CV, the service response from the Main server is transmitted to the Intermediate node. A service response message consists of two counts: data count and control count. The data count contains the number of data packets to be delivered to the CV. Control count contains the number of RTS, CTS, BUSY, ACK signal processed to transmit the request. Encryption is carried out by using PBKDF algorithm as described in Fig. 2. PBKDF algorithm takes input as data count and control count to give encrypted value as output. PBKDF algorithm encrypts the service information, so that no other nodes can access the information. It takes data count and the control count as two inputs. These two counts will be in 8-bit values. These two inputs are added and then multiplied by a value called by a function Rand(). Rand() function will generate a random value with complexity in encryption has been made. The output value is then left shifted 8 times to get the encrypted value.
- Validation phase: Fig. 3 and Fig. 4 illustrate the flow diagram for service request and reply. The encrypted value generated at the intermediate server is transmitted to the RR from which the request is forwarded. Along with the encrypted value, decryption method is also sent as a key for decryption. RR will transmit the response message to the requestor (CV). Each vehicle in the VANET has On Board Unit (OBU). The OBU will helps in validating the request message and response message. It also used in avoiding the vehicular attacks. It will decrypt the encrypted value and match the value with the VALUE send by the intermediate server. If the two values match, the service will be displayed to the user. Otherwise, the service response packets are discarded. In case of discarding of packets, retransmission takes place.

Table 2: Description of technical terms

Term	Description
CV	Client vehicle
RSU	Road side unit
SREQ	Service request
SRPY	Service reply
IS	Intermediate server
MS	Main server
EK_i	Encrypted key of $vehicle_i$
DK_i	Decrypted key of $vehicle_i$
OBU_i	On board unit of CV_i

PBKDF
{
CV_i broadcast msgid to its corresponding RSU
If CV_i needs service Send request $SREQ_i$ to RSU with msg_id
Check authorized node or not
If not authorized Discard the request and save veh_id in black list
Else Forward the request to the RSU
From RSU the request is transferred to the IS
IS validate the request
If no valid request Discard the request
Else IS records the vehicle and service information
Forwards the $SREQ_i$ to MS
MS retrieve the service and send $SRPY_i$ to IS
/* Encryption takes place in IS*/
Input the data count and control count of corresponding vehicle as 8-bit packet
Perform the function c=(a+b)*rand()
/*a is data count and b is control count*/
/*rand() function generates random value*/
For 8-bit Left shift the resultant value
The remaining value is encrypted key value EK_i
Forward the EK_i and decryption function to RSU in the region of CV_i
RSU forward the $SRPY_i$ to CV_i
/*Decryption takes place in OBU_i*/
The OBU_i performs the decryption function,
Rand()/(b-a)=c
/*a and b are data count and control count of CV_i */
Right shift the resultant value for 8-bit
The remaining value is the decrypted key value DK_i
OBU_i checks DK_i with EK_i,
If (DK_i == EK_i) Send the service to CV_i
Else Discard the service to CV_i
If needed the CV_i send the SREQ
End
}

Fig. 1: Code for PBKDF algorithm

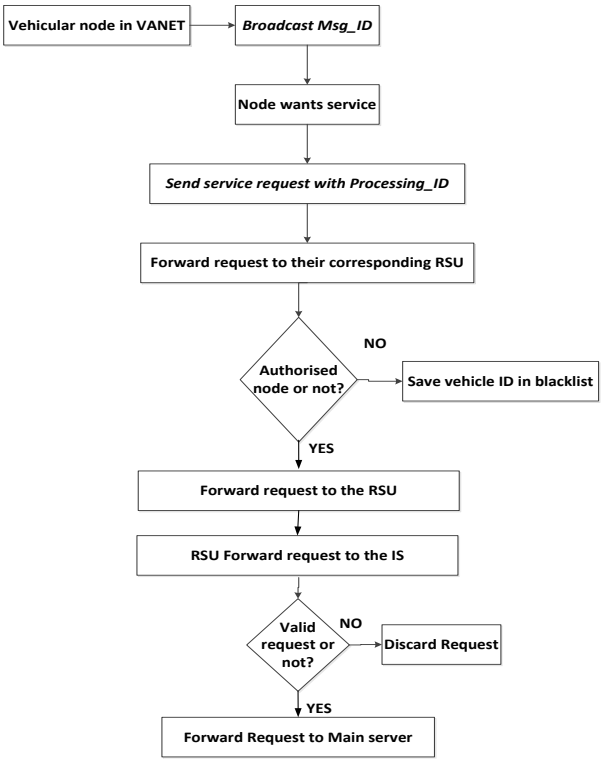

Fig. 2: Flow Diagram for service request

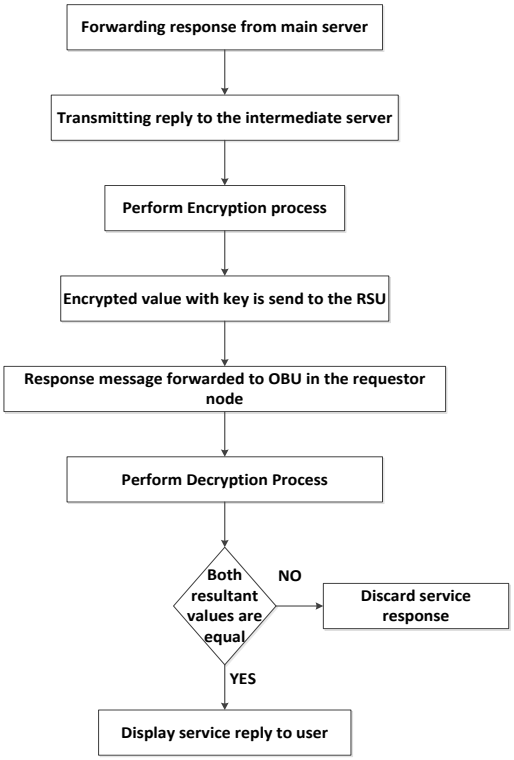

Fig. 3: Flow diagram for service reply

3. Performance analysis

Simulation of Urban Mobility (SUMO) is the microscopic, open source and multi-modal traffic simulator. The simulation allows addressing a large set of traffic management topics. Each vehicle is modelled explicitly has an own route and travel independently through the network. SUMO is coupled to a communication network simulator using a middleware called V2X Simulation Runtime Infrastructure (VSimRTI). VSimRTI is a framework which enables the groundwork and execution of V2X simulations. The easier integration and exchange of simulators enables the replacement of the most relevant simulators for a realistic presentation of traffic, communication and the execution of V2X applications. Table 3 gives the simulation parameters used in PBKDF.

Table 3: Simulation Parameters

Simulation parameters	Value
Network simulator	NS-3.19
Traffic simulator	SUMO- 0.15.0
Number of nodes	1000
Number of base station	18
MAC protocol	IEEE 802.11p
Real time environment model	Rayleigh fading environment
Connection type	CBR or UDP
IP	IPV6
Packet size	64 KB
Data rate\node	1 Mbps
CBR interval	10 Sec.
Nodes speed	Km/hr.
Gateway broadcast timer	1 Second
Antenna type	Antenna/Omni directional antenna

The proposed PBKDF framework is designed for providing privacy and security in VANET. The proposed VANET system provides security in an encrypted and decrypted form by using PBKDF which maintains the confidential information and saves the services in two ways, namely devoid of altering the information and the intruders attack. The following concludes the outcome of failure mode and effects analysis of the proposed system:

- Functional: Intermediate server can easily identify the intruders attack by using PBKDF algorithm.
- Design: As the response and reply is via the intermediate server. Intruders cannot able to alter the message.
- Process: The vehicular attacks are avoided by generating the encrypted value at the intermediate server.

4. Conclusion

In this paper, PBKDF algorithm is proposed for VANETs. This approach includes the security measures during data transmission. The architecture of proposed VANET is verified using V2X Simulation Runtime Infrastructure.

REFERENCES:

[1] P. Dharanyadevi and K. Venkatalakshmi. 2015. Potent gateway selection algorithm for integrated 3g-vmesh milieu, *World Applied Sciences J*., 33(7), 1228-1233.

[2] P. Dharanyadevi and K. Venkatalakshmi. 2015. Optimized heuristic buffer-based routing for vmesh milieu, *Australian J. Basic and Applied Sciences*, 9(11), 386-390.

[3] P. Dharanyadevi and K. Venkatalakshmi. 2014. Reliable and scalable routing protocol (RSRP) for multimedia data transmission in vehicular mesh milieu, *Int. J. Applied Engg. Research*, 9(23), 19935-19944.

[4] P. Papadimitratos, A. Kung, J. Hubaux and F. Kargl. 2006. Privacy and Identity Management for Vehicular Communication System, *Proc. Workshop on Standards for Privacy in User-Centric Identity Mgmnt.*, Zurich.

[5] S. Capkun, J. Hubaux and M. Jakobsson. 2004. *Secure and Privacy-Preserving Communication in Hybrid Ad-hoc Networks*, EPFL-IC Technical Report.

[6] A. Mishra and K. Nadkarni. 2002. Security in mobile ad-hoc networks, *The Handbook of Wireless Networks (Edited by M. Ilyas)*, Chapter 3.

[7] D. Zhou. 2003. Security issues in ad hoc networks, *The Handbook of Wireless Networks (Edited by M. Ilyas)*, Chapter 32.

[8] A. Aijaz, B. Bochow and F. Dotzer. 2006. Attacks on inter vehicle communication systems-an analysis, *Proc. 3rd Int. Workshop on Intelligent Transportation*, Hamburg, Germany.

[9] J. Blum and A. Eskandarian. 2004. The threat of intelligent collisions, *IT Professional*, 6(1), 24-29.

[10] M. Raya, P. Papadimitratos and J. Hubaux. 2006. *Securing Vehicular Communications*, EPFL.

[11] F. Dotzer. 2005. Privacy issues in VANET, *Proc. Workshop on Privacy Enhancing Technologies*, Croatia.

[12] K. Abrougui, A. Boukerche, R.W.N. Pazzi. 2011. Design and evaluation of context-aware and location-based service discovery protocols for vehicular networks, *IEEE Trans. Intelligent Transportation Systems*, 12(3), 717-735. http://dx.doi.org/10.1109/TITS.2011.2159377