International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Impact Factor (2012): 3.358

Public Key Cryptography based Secured Dynamic Routing in VANET Time Stamp based Key Management System

Shruti Bandak[1], Rekha Patil [2]

[1]M.Tech, Department of Computer Science and Engineering,
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

[2]Associate Professor and HOD, Department of Computer Science and Engineering,
Poojya Doddappa Appa College of Engineering, Gulbarga, Karnataka, India

Abstract: ***VANET is an autonomous dynamic topology network where moving vehicles exchange their position information with each other. The Selective Flooding (SF) protocol by using a brand new dynamic routing Probabilistic Broadcast (PB), Time Stamp based Key Management system (TSKMS) is proposed. It uses the key exchange protocol where multicast group header initiates a key for the group which is used to encrypt the packet such that group members can decrypt those keys. The Public Key Cryptographic method is proposed for secured transmission which is used for message authentication with Hash mechanism technique and Huffman tree. In Probabilistic Broadcast every node broadcasts packet with probability P which depends upon several parameters including bit rate, number of transmitting and receiving nodes, path loss etc. The work is simulated using Omnet++ 4.2.The simulation results are presented showing that the proposed TSKMS protocol improves the bit rate, accident duration to large extent. It also reduces the number of received packets on Onboard Unit (OBU).***

Keywords: Probabilistic Broadcast, Public Key Cryptographic, Time Stamp Key Management System, VANET.

1. Introduction

In wireless communication networks has made Inter-Vehicular Communications (IVC) and Road-Vehicle Communications (RVC) possible in Mobile Ad Hoc Networks (MANETs), this has given birth to a new type of MANET known as the Vehicular Ad Hoc Network (VANET), aiming to enable road safety, efficient driving, and infotainment.

The main criteria of VANET is that every node in a location gets the information about all the neighboring nodes in that area. Firstly, when the nodes starts to broadcast periodic messages (HELLO or Airframe) and then find a route to every independent vehicle in the area then route cache of the nodes increases many a folds with increase in number of nodes. Secondly there is no control over the topology as number of nodes changes the topology keeps on varying. Therefore in an wireless network there existing a VANET which incorporate the mobility model but does not simulate VANET in relatity.The broadcasting technique is based on notification system is developed like flooding protocol Sensor network then security messages are also broadcasted the nodes which have left the congestion area, thus making the simulation objective failed. Due to high mobility of nodes in mobile ad hoc networks, there exist frequent link breakages which lead to frequent path failures and route discoveries. The overhead of a route discovery cannot be neglected. In this paper we propose neighbor coverage based probabilistic rebroadcast protocol for reducing routing overhead in VANETs. In order to effectively exploit the neighbor coverage knowledge, we propose a novel rebroadcast delay to determine the rebroadcast order, and then we can obtain the more accurate additional coverage ratio by sensing neighbor coverage knowledge. We also define a connectivity factor to provide the node density adaptation. This approach can significantly decrease the number of retransmissions so as to reduce the routing overhead, and can also improve the routing performance. The objective is to show that by adopting proposed technique packet collision and loss at MAC layer is reduced significantly. Public Key Cryptographic techniques are energy consuming. In a specifically dynamic environment like VANET where node configuration changes frequently, assuring a secured routing is difficult. Hence we propose a time stamp constrained key exchange protocol where a multicast group header initiates a key for the group which is used to encrypt the packet such that group members can decrypt them.

Important deviation of our approach from other VANET protocols is that nodes in proposed protocol acts as autonomous entity and does not join or form any multicasting group thus reducing Multicast overhead. The time based key ensures that keys are changed frequently enough to keep the intruder guessing. Further it limits the necessity of key exchange rate that can dissipate huge node energy.

2. Organization

This paper is organized as follows, section 1 discusses the introduction and section 3 describes related work. Section 4 details the system design and implementation. Section 5, presents the performance evaluations of our system design. Finally, section 6 presents some concluding remark.

3. Related Work

Vehicular Ad Hoc Networks (VANETs). In these networks, vehicles communicate with each other and possibly with a roadside infrastructure to provide a long list of applications varying from transit safety to driver assistance and Internet access. Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems the author Horacio , Oliveira , Eduardo F. Nakamura,Antonio A.F. Loureiro [1], has described these networks, knowledge of the real-time position of nodes is an assumption made by most protocols, algorithms, and applications and discuss the subject by studying and analyzing the localization requirements of the main VANET applications. VANET: "Routing Protocols, Security Issues and Simulation Tools", Mushtak Y, Gadkari1and Nitin B [2], author has proposed a Vehicular ad hoc network is of searching and maintaining an effective route for transporting data information. Security and privacy are indispensable in vehicular communications for successful acceptance and deployment of such a technology. Simulator tool has been preferred over outdoor experiment because it simple, easy and cheap. Patrick I. [3] has discussed, the network's challenges lie on its capacity for information system confidentiality (the prevention of unauthorized disclosure), integrity (the prevention of the unauthorized modification), availability (the prevention of unauthorized suppression of data or resources), stable communication in the presence of highly mobile nodes, and privacy concerns. GhassanSamara and Wafaa A.H.alsalihy [4] has analyzed and discussed the various dimensions of VANETs security including security threats, challenges in providing security in vehicular networks environment, requirements and attributes of security solutions. Saira Gillani, Farrukh Shahzad, and Amir Qayyum [5]has presented ,the various dimensions of VANETs security including security threats, challenges in providing security in vehicular networks environment, requirements and attributes of security solutions and also provide taxonomy and critically review of the notable security solutions – available for VANETs in literature Ramanpreet Kaur and Er. Khyati Marwaha [6] has proposed the effect of varying speed of vehicles on security protocol with on behalf of different routing protocols. The performance of VANETs will be analyzed on behalf of metrics like Throughput and End-to-End Delay. P.Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl, [7] has described the emerging technology of vehicular communications (VC) raises a number of technical problems that need to be addressed. Author identifies VC-specific issues and challenges, considering the salient features of these systems. J.P. Hubaux [8] has proposed about road safety, traffic management, and driver convenience continues to improve, in large part thanks to appropriate usage of information technology. But this evolution has deep implications for security and privacy. M. Scott [9] have presented a fast method for calculation of the Tate pairing, as required for pairing- based cryptographic protocols. Author points out various optimizations and tricks, and compare timings of a pairing-based Identity Based Encryption scheme with an optimized RSA implementation. Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su [10] has proposed an efficient pseudonymous authentication scheme with strong privacy preservation (PASS), for vehicular communications. Extensive simulations demonstrate that PASS outperforms previously reported schemes in terms of the revocation cost and the certificate updating overhead.

4. Methodology

The basic objective of VANET is that all the nodes should be able to gather information about position of all the neighboring nodes. Based on position information of other nodes, can be determined on the course of action like changing route or changing speed and so on. We propose a novel rebroadcast delay to determine the rebroadcast order, and then we can obtain the more accurate additional coverage ratio by sensing neighbor coverage knowledge.

4.1 Proposed System

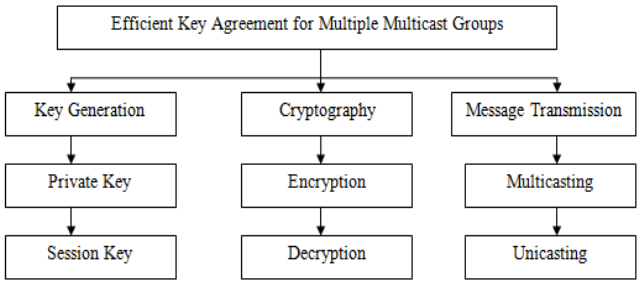


Figure 1: Architecture of the proposed system

4.2 Message transmission

Multicasting is a process of sending a message to a selected group. Internet applications, such as online games, newscast, stock quotes, multiparty conferences, and military communications can benefit from secure multicast communications. In most of these applications, users typically receive identical information from a single or multiple senders. Hence, grouping these users into a single multicast group and providing a common session encryption key to all of them will reduce the number of message units to be encrypted by the senders. Various types of data communication are broadcast, Multicast, group communication.

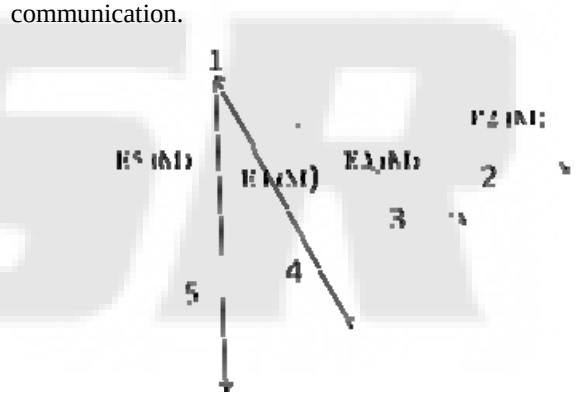


Figure 2: Transmission of the message M through 4 point-to-point connections

The above fig1 shows, the transmission of message m to four point to point connections. Here node number 1 is the service provider. Nodes 2,3,4,5 are the receiving nodes. Nodes 2,3,4,5 are receiving the same message.

4.3. Group communication

For group communications, the server distributes to each member a group key to be shared by all members of the group, distributing the group key securely to all members requires messages encrypted with individual keys (a computation cost proportional to group size). Each such message may be sent separately via uncast. Alternatively, the messages may be sent as a combined message to all group members via multicast. Either way, there is a communication cost proportional to group size (measured in terms of the number of messages or the size of the combined message). Observe that for a point-to-point session, the costs of session establishment and key distribution are incurred just once, at the beginning of the session. A group session, on the other hand, may persist for a relatively long time with members joining and leaving the session. Consequently, the group key should be changed frequently. To achieve a high level of security, the group key should be changed after every join and leave so that a former group member has no access to current communications and a new member has no access to previous communication.

4.4. Authentication

Authenticity means that when a user receives a message, it is assured about the identity of the sender. The authenticity requirement can be translated in the context of secure multicast into two requirements on key and data distribution.

- **Key authenticity:** Only the center can generate a session key.
- **Data authenticity:** The users can distinguish among the data sent by the center and the malicious data sent by an attacker.

4.5. Algorithm

Step 1: Location prediction:

- Predict location information (*<x,y>*) over the next *"I"* beacons
- Construct a prediction table for each beacon.

Table 1: Probability of each beacon

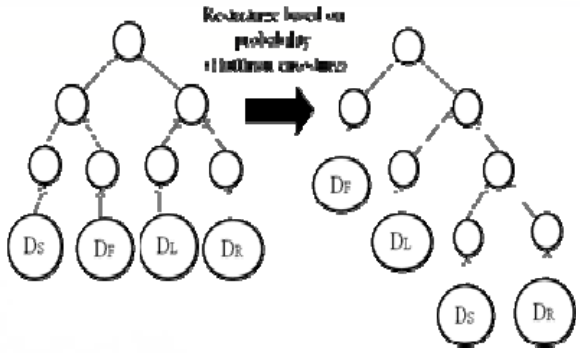
Possible Movement (L_i-L_{i-1})	Probability
Stay(Ds)	?
Forward(Df)	?
Forward left(Dl)	?
Forwardright(Dr)	?

Step 2: Time Stamp Bound:

- Makes use of Huffman coding for generating air frame messages (Hello).
- Construct Huffman binary tree for each beacon.
- Chain the " I " Huffman trees for the " I " beacons to form a Chained Huffman tree (CHT).
- The root of the CHT is for the authentication of the " I " beacons.

Table 2: Probability of authentication beacons

Possible Movement (L_i-L_{i-1})	Probability
Stay(Ds)	P_S
Forward(Df)	P_F
Forward left(Dl)	P_L
Forwardright(Dr)	P_R



Step 3: Message Broadcast:

- Commitment of the tree must be authenticated to all receivers via the generated pseudonyms.
- Send first beacon

$B_0 = \{m_0, S(m_0), cert\}$ *where* ,
$m_0 = \{T_0, L_0, (dx,dy)\}$

After commitment is authenticated, send "m_i" and off-path values as the Message.

Step 4: End.

4.6. Block Diagram

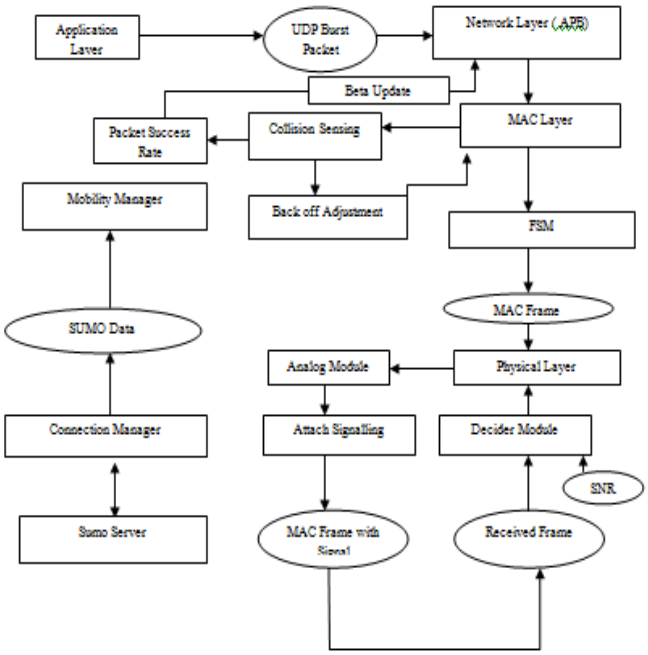


Figure 3: Flow diagram of packet routing

In the above flow diagram sumo is connected to omnet++through TCP connection manager. Application packet is forwarded to Network layer. We use Probabilistic Broadcast and Adaptive Probabilistic broadcast for routing. Network layer protocol is changed in Car.ned .When the module receives data from Application layer it invokes

handle Upper Message and insert the message into a broadcast queue. Probabilistic Broadcast checks the Beta values returned by Adaptive Probabilistic Broadcast. If beta value satisfies current probability saturation using Bernoulli then packet is sent else it is down. If routing is selected as only Probabilistic Broadcast then beta value remains constant and packets are always transmitted with fixed probability and at equal interval of time. We define CSMA MAC layer. It is best effort MAC. CSMA is like slotted Aloha but has the capability to back off suitably when a collision is detected. Its operation is also divided into two methods: handle Upper Message where the layer transmits network layer packet through physical radio. Handle Lower Message is one through which node receives signals coming from other nodes through radio interface and forwards it to Network layer. Note that MAC implements fair scheduling which determines the transmission schedule of the messages based on signal to interference ratio and does it through FSM module. It also registers Number of Received and Transmitted frames as performance parameters. MAC is connected to Physical layer which is Physical radio model.

Omnet is basically a packet based simulator and physical layer is all about signaling. Omnet simulation creates a special field in the packet called signal and implements the physical signaling. All the modulation and loss is implemented in this signaling. Through Configuration file simulation must be given an Analog module as Input.Config.xml which is given as input to the simulation through omnetpp.ini using manager section. It defines the loss model and decider module. A decider module is one which upon receiving any signal checks if signal meets SINR threshold or not. If not then it drops the signal. Extraction of signaling part from MAC frame is implemented in all the deciders in following way. Base Decider it can be seen that Decider first extracts the signal part from the packet. Then it gets the signal power and noise map. It calculates reception power. From reception power, noise power, signal power can be calculated and from signal power and noise power SNR is calculated. Once Physical module gets any new frame, it processes that through decider module and signal reception success is determined. Sensitivity is noise cancellation capability of the receiver electronics and its typical value is -84dBm. However more noise cancellation needs more power. Thus sensitivity can be varied while checking network performance.

5. Results

5.1. Simulation parameters

Table 3: Simulation Parameters

Parameters	Value
Simulator	OMNET 4.2, SUMO
MAC protocol	IEEE 802.11p
Average SNR	-84dB
Number of Vehicles	100
Simulation Time	1000s
MaxTransmission Power	100mW
Header Length	24bit
Burst Size	10

In the fig 4, as the simulation time increases, as the number of data packet forwarded and number of data packet received also increases at the application layer and it comes to stable during the simulation time 500s and remain constant. Hence by comparing the graphs of Selective Flooding (SF) with proposed system the Probabilistic Broadcast (PB) is more efficient in forwarding the application packet.

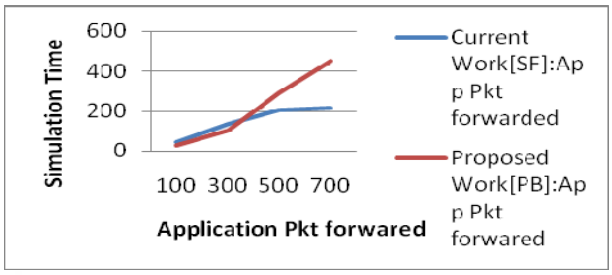


Figure 4:Simulation Time Vs Application Pkt forwared

In the fig 5, the end to end delay increases in the application layer the number of received on OBU packets also increases and later reaches the constant level. Hence by comparing the graphs of Selective Flooding with Proposed system the Probabilistic Broadcast is more efficient in forwarding the application packet.

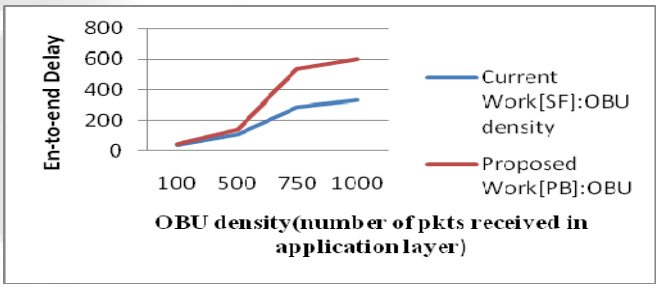


Figure 5:End-to-End delay Vs OBU density

In the fig 6, as the simulation time increases, the message loss ratio increases up to 250s in proposed system by Probabilistic Broadcast (PB). But whereas the Current system by Selective Flooding (SF) the message loss ratio decreases thus there will be no transmission of packets further.

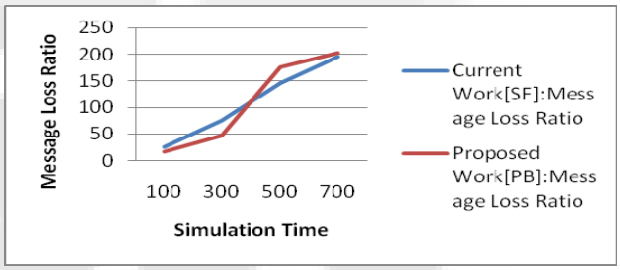


Figure 6: Average number of Message Ratio Vs Simulation Time

In the fig 7, bit rate is number of bits transmitted per second. As the bit rate increases the packet delivery ratio also increases. At 512bps PDR start decreasing because of congestion clearance in the network so, Optimum value is above 5000bps.

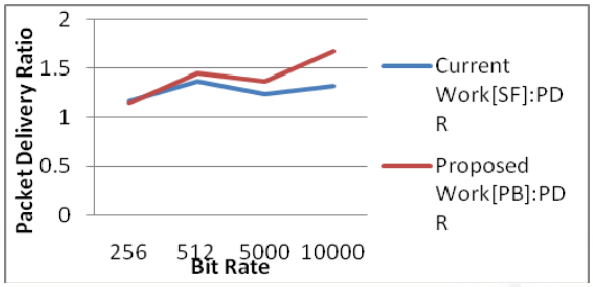


Figure 7: Packet Delivery Ratio Vs Bit Rate

In the fig 8 and fig 9,accident duration decreases at the number of received packect.As simulation time increases the carbon di oxide footprints also increases because has the more number of vehicles enters the playground area of Omnet++ and also the collison of packets occurs.So the delay will simultaneously increases in the current and proposed work.

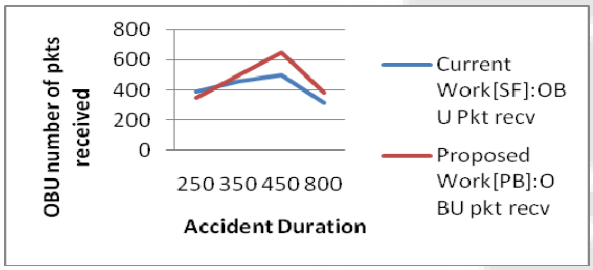


Figure 8: Accident Duration Vs OBU number of pkts received

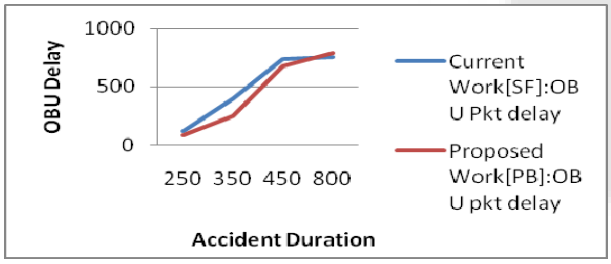


Figure 9: OBU pkt delay Vs Accident Duration

6. Conclusion and Future Work

VANET plays a different role as information exchange goals is to dissipate information from one node to maximum number of nodes. The proposed dynamic routing Probabilistic Broadcast which shows the simulation results of bit rate, number of transmitting and receiving nodes, message loss ratio, end-to-end delay, accident duration etc. Through this simulation by comparing the proposed work with the Current system reduces speed variability to a great deal and in Adaptive Probabilistic Broadcast, the network packet congestion is reduced through secured communication technique “Public Key Cryptographic using Time Stamp Key Management System” which also minimize Collision in MAC and delay.

Future Work: The future work focuses on making our proposed more scalable in terms of number of users that can connect to an RSU. By this method, we can priorities the Time Slots for each user and hence the messages on RSU can be distributed equally.

References

[1] Vehicular Ad Hoc Networks: A New Challenge for Localization-Based Systems” Q Azzedine Boukerche a,*, Horacio A.B.F. Oliveira a,b,c, Eduardo F. Nakamura b,d,Antonio A.F. Loureiro Computer Communications xxx (2008) xxx–xxx

[2] Mushtak Y. Gadkari1, Nitin B. Sambre2 “VANET:Routing Protocols, Security Issues and Simulation Tools” IOSR Journal of Computer Engineering (IOSRJCE) ISSN: 2278-0661 Volume 3, Issue 3 (July-Aug. 2012), PP 28-38 Page.

[3] Patrick I. Offor Nova Southeastern University”Vehicle Ad Hoc Network (VANET): Safety Benefits and Securitychallenges” po125@nova.edu

[4] GhassanSamara#1,WafaaA.H.alsalihy*2,rsures# “Security Analysis of Vehicular Ad Hoc Networks”(VANET) 2010 Second International Conference on Network Applications, Protocols and Services.

[5] Saira Gillani, Farrukh Shahzad, Amir Qayyum, “A Survey on Security in Vehicular Ad Hoc Networks”

[6] Ramanpreet Kaur1, Er. Khyati Marwaha “Analysing the effect of Speed on Security Protocol in VANETS” International Journal ofAdvanced Research in Computer and Communication EngineeringVol. 2, Issue 8, August 2013.

[7] P.Papadimitratos, A. Kung, J.P. Hubaux, and F. Kargl,“Privacyand Identity Management for Vehicular Communication Systems:A Position Paper,” Proc.Workshop Standards for Privacy in User-Center Identity Management, July 2006.

[8] J.P. Hubaux, “The Security and Privacy of Smart Vehicles,” IEEE Security and Privacy, vol. 2, no. 3, pp 49-55, May/June 2004.

[9] M. Scott, “Computing the Tate Pairing,” Proc. Int’l Conf. Topics in Cryptology, pp. 293-304, 2005.

[10] Y. Sun, R. Lu, X. Lin, X. Shen, and J. Su, “An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications,” IEEE Trans.Vechicular Technology,vol.59,no7,pp.3589-3 Sept.2010.