The Edsrc in Vannet for Cooperative Video Streaming

A. Samayadevi, A. Aarthi
PREC, Thanjavur,
Tamilnadu

***Abstract*-- Enhanced Vehicular ad hoc networks (EVANNETs) have attracted extensive attentions recently as a promising technology for revolutionizing the transportation systems and providing broadband communication services to vehicles. EVANNETs consist of entities including Enhanced On-Board Units (EOBUs) and infrastructure Enhanced Road-Side Units (ERSUs). Enhanced Vehicle-to- Vehicle (EV2V) and Enhanced Vehicle-to-Infrastructure (EV2I) communications are the two basic communication modes, which, respectively, allow EOBUs to communicate with each other and with the infrastructure RSUs. Since vehicles communicate through wireless channels, causes performance and security issues. For Example consider accommodating Video stream in Enhanced VANNET leads to time delay and lack in performance. We Proposed a EEDSRC protocol that implies 1) Streaming Task assignment schedule the streaming task to each member in cooperative network and packet Forwarding Strategy to the requested member to upgrade performance 2) Efficient certificate revocation checking process to upgrade security. From the Experimental result the proposed scheme highly relies on the up gradation in security and performance over Hybrid Enhanced VANNET in Cooperative transmission.**

Key words: EVANNET, Video Streaming, EEDSRC

I INTRODUCTION

Vehicular ad hoc networks (EVANNETs) have attracted wide-ranging politeness recently as a hopeful technology for revolutionizing the transportation systems and provided that broadband announcement services to vehicles. EVANNETs consist of entity including Enhanced On-Board Units (EOBUs) and infrastructure Enhanced Road-Side Units (ERSUs). Enhanced Vehicle-to- Vehicle (EV2V) and Enhanced Vehicle to-Infrastructure (EV2I) transportation are the two basic communication modes, which, respectively, allow EOBUs to communicate with each other and with the infrastructure ERSUs. Since vehicles communicate through wireless channels, a variety of attacks such as injecting false information, modifying and replaying the distributed post can be easily launched. A security attack on EVANNETs can have brutal hurtful or fatal consequences to justifiable users. Consequently, ensuring strong vehicular connections is a must before any EVANNET application can be put into practice.

A. EVANNET AND EOBU

A well-recognized solution to secure EVANNETs is to deploy Enhanced Public Key Infrastructure (EPKI), and to use Enhanced Certificate Revocation Lists (ECRLs) for managing the revoked certificates. In EPKI, each entity in the network holds an authentic certificate, and every message must be digitally sign prior to its program A ECRL, usually issued by a Enhanced Trusted Authority (ETA), is a list containing all the revoked certificates. In a EPKI system, the substantiation of several message is perform by first checking if the sender's certificate is included in the current ECRL, i.e., scrutiny its revocation status, then, verify the sender's certificate, and finally verify the sender's autograph on the received message. The first part of the substantiation which checks the revocation status of the sender in a ECRL, may incur lengthy setback depending on the ECRL size and the employed mechanism for searching the ECRL. Unfortunately, the ECRL size in EVANNETs is expected to be large for the following reasons: 1) To save the retreat of the drivers, i.e., to abstain the seepage of the existent identity furthermore setting in rank of the drivers from any external eavesdropper each EOBU should be preloaded with a set of anonymous digital certificates, where the EOBU has to periodically change its anonymous certificate to mislead attackers. Consequently, a revocation of an EOBU results in revoking all the certificates carried by that EOBU leading to a large increased in the ECRL size. 2) The scale of EVANNET is very large. According to the United States Bureau of Transit Statistics, there are approximately 240 million EOBUs in the Unites States in 2010.Since the number of the EOBUs is huge and each EOBU has a set of certificates, the ECRL size will increase dramatically if only a small portion of the EOBUs is revoked. To have an ideas of how large the ECRL size can be, consider the case where only 100 EOBUs are revoke and each EOBU has certificate. In this case, the ECRL contains 2.55 million revoked certificates. According to the employed mechanism for searching a ECRL, the Wireless Access in Vehicular Environments (EWAVE) standard does not state that either a non optimized searched algorithm, e.g., linearly search, or some sorts of optimized searching algorithm such as bizarrely search, will be used for searching a ECRL. In this paper, we consider both non optimized and optimized search algorithms. According to the Enhanced Dedicated Short Range Communication (EDSRC), which is part of the EWAVE standard, each EOBU has to broadcast a message every 3000 msecs about its location, velocity, and other telematics information.

In such scenario, each EOBU may be given a large number of messages every 3000 msecs, and it has to check the recent ECRL for all the received certificates, which may incur extensive authentication delay depending on the ECRL size and the number of received certificates. The ability to check a ECRL for a large number of certificates in a timely manner leads an to be anticipated challenge to EVANNETs. To ensure reliable operation of EVANNETs and increase the amount of authentic in sequence gained from the received messages, each EOBU should be able to check the revocation status of all the received certificates in a timely manner. Most of the existing works overlooked the authentication delay resulting from checking the ECRL for each received certificate. In this paper, we introduce an enhanced expedite message authentication protocol1 (EEMAP) which replaces the ECRL scrutiny process by an efficient revocation checking process using a fast and secure EHMAC function. EEMAP is suitable not only for EVANNETs but also for any network employing a EPKI system. To the best of our knowledge, this is the first solution to reduce the substantiation delay resulting from scrutiny the ECRL in EVANNETs.

Streaming Media may be defined as listening or viewing media in real time as it comes across the World Wide Web. With streaming technology, users can watch and listen to media while it is being sent to their browser, instead of waiting for it to completely download and then playing it. Before streaming technology was available, a user might wait an hour to completely download a short media file. In general, media files are huge. For example, five minutes of uncompressed video would require almost one gigabyte of space. So, when the audio and video is prepared for streaming, the media file is compressed to make the file size smaller. When a user requests the file, the compressed file is sent from the video server in a steady torrent and is decompressed by a steaming media player on the user's computer to play automatically in real time. A user can jump to any location in the video or audio presentation. Streaming media generally tries keep pace with the user's connection speed in order to reduce interruptions and stalling. Though general network blockage is unavoidable, the streaming server attempts to compensate by maintaining a regular connection.

II PROJECTED WORK

In the proposed system, EEMAP can be used for the authentication purposes and the time delay can be decreased. In the wireless system for the connection purpose or data sharing purposes instead of using ECRL here we use fast and secure EHMAC function for authentication purposes. This is the first process to reduce the authentication delay in the EVANNET Network. The EOBU units can maintain the secret keys and it can be communicate with ERSU for keep posted the secret keys. The EOBU fixed into the vehicle and it can be commune with ERSU or other EOBU and it can be communicate continuously. In the EOBU onwards having the security dilemma means checking the pressure by enhanced Trusted Authority.

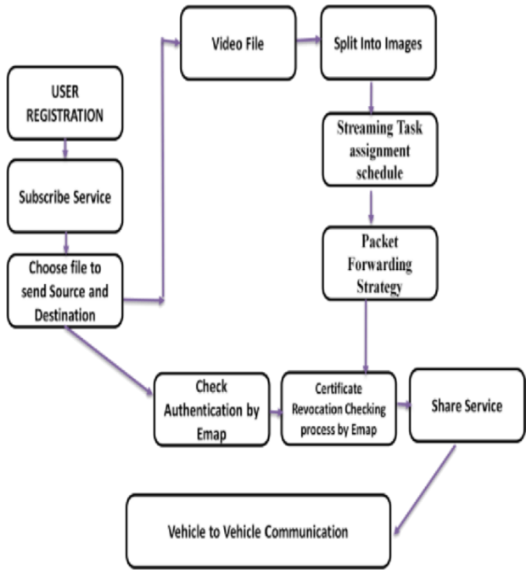

Fig 1: Overall Process of Block Diagram

If a person wants to send a file they must register in the User registration. Then only they have to Enhanced Subscribe the service. After that they have to choose the file to reach the destination from the source. If it is the video file means, first it will be split into images. For that process it have two algorithms. One is Streaming task assignment schedule and another one is Packet forwarding strategy. First it will be check the authentication by EEMAP It will be correct means it will share service from one vehicle to another vehicle.

III UML DIAGRAM

The user,first register in the network, then they have to subscribe the service. For this two processes makes faster, they have use the EEMAP. The user and the EEMAP verify the authentication and then accessing the services.

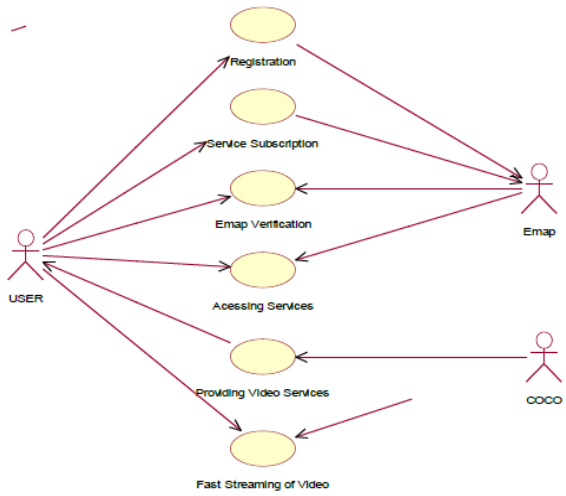

Fig 2: UML diagram

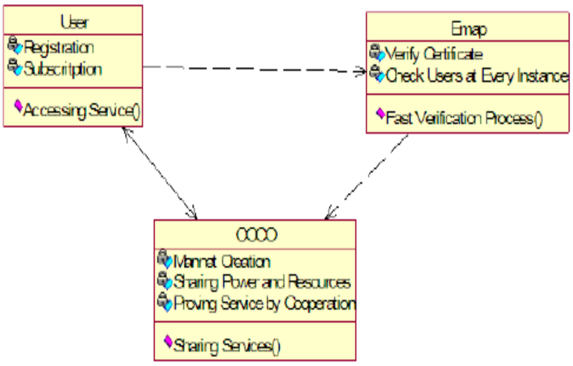

Fig 3: Class Diagram

This is the class diagram, it has the same three processes user,eemap and coco.

Sequence diagram helps to show the activity of objects in a use case by describing the object in this sequence.

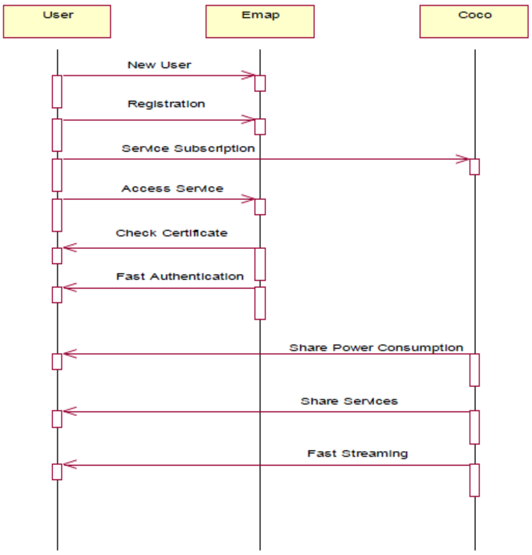

Fig 4: Sequence Diagram

The collaboration diagram shows the relationship between objects and the order of messages passed between them.

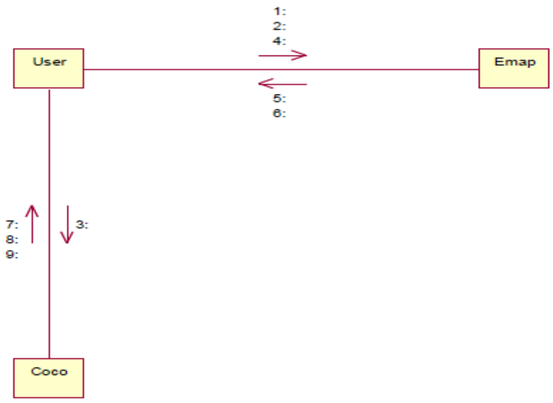

Fig 5: Collaboration Diagram

IV FLOW CHART

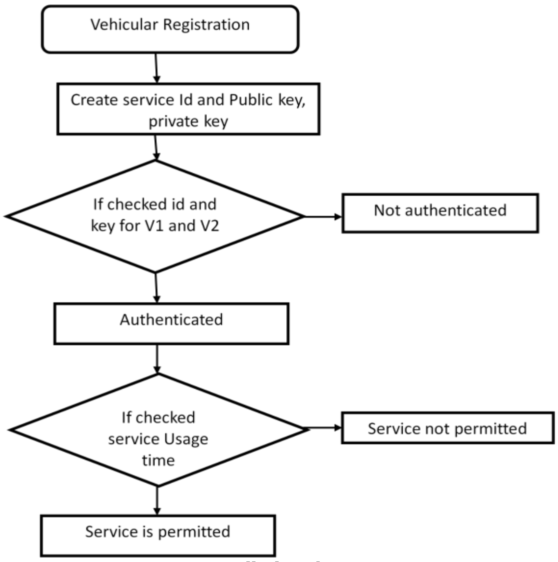

Fig 6: Overall Flowchart Process

V ALGORITHMS EEMAP

1: Check the validity of Tstamp
2: if invalid then
3: Drop the message
4: else
5: Check REVcheck¼ ?HMACðKg; PIDukTstampÞ
6: if invalid then
7: Drop the message
8: else
9: Verify the TA signature on certOBUu
10: if invalid then
11: Drop the message
12: else
13: Verify the signature siguðMkTstampÞusing OBUupublic key ðPKuÞ
14: if invalid then
15: Drop the message
16: else
17: Process the message
18: end if
19: end if
20: end if
21: end if

VI SIMULATION RESULT

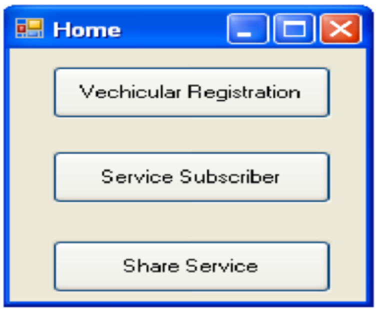

Fig 7:EEMAP

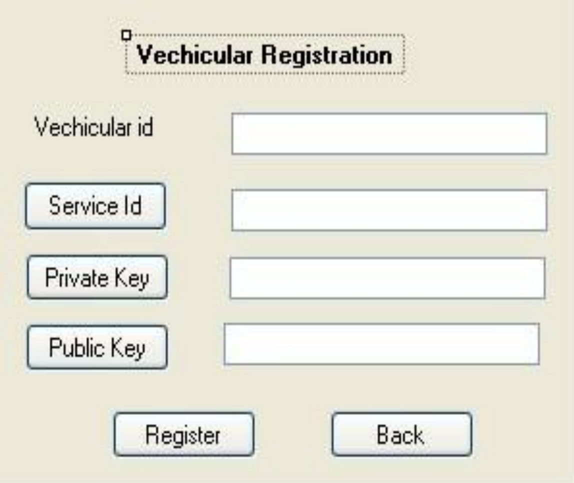

Fig 8: VEHICULAR REGISTRATION

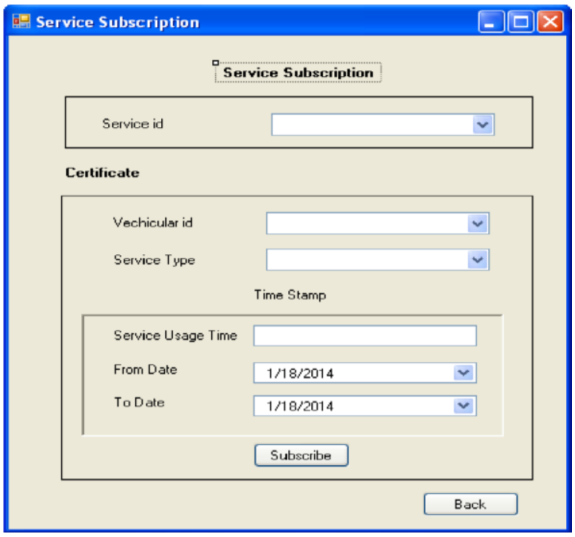

Fig 9: SERVICE SUBSCRIBER

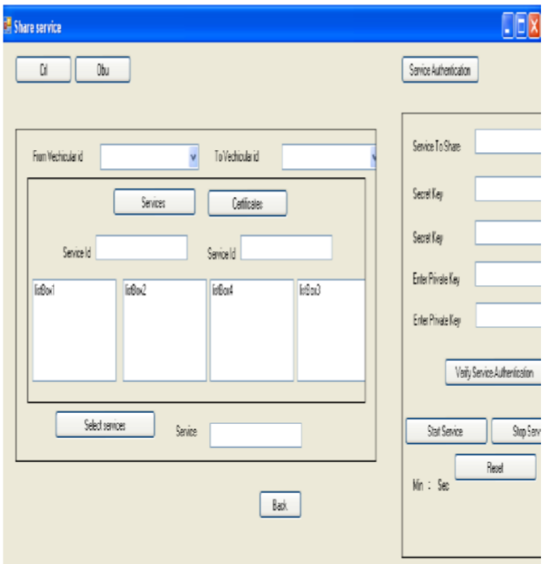

Fig 10: SHARE SERVICES

Fig 11: VIDEO STREAMING-TRANSMITTER

Fig 12: VIDEO STREAMING –RECEIVER

VII CONCLUSION AND FUTURE ENHANCEMENT

ECRL checking process with a fast revocation checking process employing EHMAC function. The proposed EEMAP uses a novel key sharing mechanism which allows an EOBU to update its compromise keys even if it before missed some revocation messages. The EVANNET is created and EOBU created for communiqué. Key bent for secure communiqué Our future work will focus on the credential and message signature substantiation acceleration. In this System, the key in giving out can be checked in the ECRL and the cost can be evaluate to maintain the EOBU system the memo ratio and message verification cannot be equal and the memo ratio can be continuously increased and it can be controlled by using available ECRL and the memo cannot be more then the request message in the wireless system.

REFERENCES

[1] Privacy-aware route tracing and revocation games in VANET-based clouds “Hussain, R. ; Dept. of omput. Sci. & Eng., Hanyang Univ., Seoul, South Korea ; Abbas, F. ; Junngab Son ; Hasoo Eun” Published in: Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on Date of Conference: 7-9 Oct. 2013 Page(s): 730 – 735

[2] Comparation of Strategies for Data Replication in VANETEnvironment“Janech, J. ; Lieskovsky, A. ; Krsak, E.” Advanced Information Networking and Applications Workshops (WAINA), 2012 26th International Conference on DOI: 10.1109/WAINA.2012.179 Publication Year: 2012 , Page(s): 575 - 580

[3] SDMA: On The Suitability for VANET”Xianbo Chen ; Refai, “H.H. Information and Communication Technologies: From Theory to Applications, 2008. ICTTA 2008. 3rd International Conference on DOI: 10.1109/ICTTA.2008.4530188 Publication Year: 2008, Page(s): 1 -5

[4] A Priority Selected Cache Algorithm for Video Relay inStreaming Applications”Shin-Hung Chang ; Ray-I Chang ; Jan-Ming Ho ; Yen-Jen Oyang “Broadcasting, IEEE Transactions on Volume: 53 , Issue: 1, Part: 1 DOI: 10.1109/TBC.2006.887170 Publication Year: 2007 , Page(s): 79 - 91

[5] V3: a vehicle-to-vehicle live video streaming architecture”Meng Guo ; Ammar, M.H. ; Zegura, E.W. “Pervasive Computing and Communications, 2005. PerCom 2005. Third IEEE International Conference on DOI: 10.1109/PERCOM.2005.53 Publication Year: 2005 , Page(s): 171 - 180

[6] Video quality assessment in video streaming services considering user preference for video content”Rodrriguez, D. ; Rosa, R. ; Costa, E. ; Abrahao, J. ; Bressan, G. “Consumer Electronics, IEEE Transactions on Volume: 60 , Issue: 3 DOI: 10.1109/TCE.2014.6937328 Publication Year: 2014 , Page(s): 436 – 444

[7] Study of the Feasibility of VANET and its Routing Protocols”Sun Xi ; Xia-Miao Li “Wireless Communications, Networking and Mobile Computing, 2008. WiCOM '08. 4th International Conference on DOI: 10.1109/WiCom.2008.1021 Publication Year: 2008 , Page(s): 1 - 4

[8] Scalable Wireless Video Streaming over Real-Time Publish Subscribe Protocol (RTPS)”Al-Madani, B. ; Al-Saeedi, M. ; Al-Roubaiey, A.A. “Distributed Simulation and Real Time Applications (DS-RT), 2013 IEEE/ACM 17th International Symposium on DOI: 10.1109/DS-RT.2013.32 Publication Year: 2013 , Page(s): 221 – 230

[9] Comparison of traffic and quality characteristics of rate-controlled wavelet and DCT video”Kulapala, B. ; Seeling, P. ; Reisslein, M. “Computer Communications and Networks, 2004. ICCCN 2004. Proceedings. 13th International Conference on DOI: 10.1109/ICCCN.2004.1401638 Publication Year: 2004 , Page(s): 247 – 252

[10] Encoding stored video for streaming applications”Pao, I.-M. ; Ming-Ting Sun “Circuits and Systems for Video Technology, IEEE Transactions on Volume: 11, Issue: 2 DOI: 10.1109/76.905985 Publication Year: 2001 , Page(s): 199 - 209