HAP: Hybrid Authentication Protocol for Vehicular Ad Hoc Network

Manish Kumar Soni
Research Scholar
IET Alwar,

Ashish Vashistha
Dept. CSE
IET Alwar,

ABSTRACT
In vehicular ad hoc networks clever traffic services are efficient if they are connected with method that supervise and create trust among service providers and vehicles. Consequently, the authentication of the providers of traffic condition information and the authorization of entity's to admittance this information is crucial. Consequently it's essential to extend a innovative security scheme for VANETs protocol.

General Terms
In this paper we proposed improves the security of location-based routing (LBR) protocols. This clarification can defy nearly each of the attacks, still those attacks which at present accessible security protocol can't treaty among, such as the maliciously drop-packets-attack like black hole attack, a system is proposed to improve the security concert of LBR protocols.. This method has prove efficiency and has better security.

Keywords
VANETs; authentication, certificate status information, BR protocols.

1. INTRODUCTION
On the other hand, intelligent traffic services are effective if they are associated with mechanisms that manage and establish trust between service providers and vehicles. In VANETs, they must be accompanied by efficient mechanisms for certificate revocation and validation.

Thus it's necessary to develop a new security scheme for VANETs protocol. Among all the routing protocols of VANETs, the protocols based on location are better than other category on network performance, and the algorism is simpler. A secure enhanced location-based protocol is proposed in this paper. It improves the security of location-based protocol. This solution can resist almost all of the attacks, even those attacks which currently existing security protocol can not deal with such maliciously drop packets attack like black hole. Furthermore, out-of-band attack like Since VANETs have great potential in improving the traffic condition and location -based protocol is popular in VANETs, a method is proposed to expand the security performances of location-based routing protocols. Like other security solutions, this scheme employs digital signature to guarantee the identity authentication, data integrity and no denial. The difference to most of other existed solutions is that an evaluation mechanism is proposed, which can detect malicious nodes that drop or tamper routing data. This mechanism has been proved efficiency and has better security and network performance by comparing with the hybrid signature routing scheme. In this paper we proposed improves the security of location-based routing (LBR) protocols. This clarification can defy nearly each of the attacks, still those attacks which at present accessible security protocol can't treaty among, such as the maliciously drop-packets-attack like black hole attack, a system is proposed to improve the security concert of LBR protocols.. This method has prove efficiency and has better security. The paper is organized as follows. Section II reviews the related work. Section III approach authentication requirements. Section IV hybrid authentication protocol. Section V concludes the paper.

II. RELATED WORK
Through classify to authenticate security messages in vehicular ad hoc networks, plenty of methods have been proposed. Diminutive of the studies have addressed the problem of Subir Biswas, Jelena Misi c they present an anonymous authentication scheme for vehicular networks that provides conditional anonymity to collocated vehicles. A modified ECDSA mechanism utilizes the position information of vehicles operating together in close proximity for generation and verification of elliptic curve based signatures on safety and other application messages. This waives the requirement of a third party public-key certificate for message authentication in VANET. Their scheme provides a privacy-preserving, lightweight, secure and compatible instant authentication for vehicle-originated safety messages. Security analysis and simulation experiments justify the usefulness of our scheme .Yu-Chih Wei,Yi-Ming Chen Hwai-Ling Shan, in this paper, they propose a trust scheme which aims to thwart internal attackers in privacy enhanced VANETS. In the proposed scheme a secure broadcast authentication protocol and beacon-based trust management system are being employed to maintain the trustworthiness of vehicles. they adopt Dempster-Shafer Theory to incorporate trustworthiness of event message with vehicle trustworthiness from multiple vehicles. In order to ensure the reliability of the proposed scheme, they evaluate the performance under alteration and denial-of service attack models. The simulation results proposed system is highly resilient to adversary attacks no matter whether it is under fixed silent period (FSP) scheme or random silent period (RSP) location privacy enhancement scheme. Debasis Giri and Durbadal Chattaraj.The most important research challenge is the authentication of VANET messages with less communication as well as storage overhead. In this paper, they was introduce an infrastructure oriented (RSU-aided or road side unit aided) message authentication scheme named IOMAS with less communication and storage overhead compared to the previously published scheme. In the proposed scheme, an RSU takes the responsibility for verifying the incoming messages from vehicles and transmits the response back to the vehicles with less communication cost Raya et al. addressed the problem of conditional privacy in VANETs by using a

huge set of time-specified short lived certificates preloaded in each vehicle at the time of registration. Since each vehicle is preloaded with much more anonymous certificates than it would possibly use, the certificate authority would require a rigorous searching effort once a user identity has to be traced out. Also, a key revocation consumes significant bandwidth as the size of the revocation list grows. The problem of key revocation in anonymous certificate based authentications has been resolved by Sun et al. where the size of the revocation list is kept linear with the number of revoked nodes using a one-way hash function based mechanism. In order to provide vehicular anonymity, an OBU updates its pre-loaded TA certificates by re-signing them with new keys from RSU. This makes an RSU a potential subject to a node compromise attack. Lin et al. used the combination of group signature and ID-based signature scheme for vehicular anonymous authentication, while Wu et al. proposed a message linkable group signature (MLGS) for thwarting sybil attacks in privacy preserving vehicular communications. A hybrid scheme for VANET authentication combines the concept of anonymous certificate scheme with the group signature scheme in. Instead of signing a message directly, a group signing key certifies node's self-generated pseudonyms. The group signature and verification mechanism ensures that the certificate was issued by a registered member of the certificate authority. A similar approach by Lu et al. provides resilience to the RSU compromise attacks, while it requires multiple handshaking between OBUs and RSUs for a bilinear pairing based mutual authentication scheme. Both Sun et al. and Lu et al. are functional only under proper RSU coverage in the network. Bilinear pairings operations are expensive in terms of computation time and complexity. Also, most typical and frequently made pairing assumptions are not feasible in practice. A discrete logarithm and hash function-based solution to VANET authentication has been proposed in. However, discrete logarithm based signature schemes require larger keys (more than 512 bits) for signature generation and verification; hence, incur higher computation costs compared to other schemes (e.g. Elliptic curve cryptosystems) with equivalent security strength. While Efficient Security Scheme for Position-Based Routing in Vehicular Ad Hoc Networks (ESPR)], of which the security mechanism mainly employs the HMAC to achieve secure operation between intermediate nodes, still employs digital signature between end-to-end protections. Comparing with the hybrid signature scheme, it is more efficient because the cost of doing HMAC is less than doing digital signature. GPSR: Greedy Perimeter Stateless Routing for Wireless Networks proposed a position-based protocol in detail. GPRS is a classic position-based routing protocol, into which we applied our scheme.

III. APPROACH AUTHENTICATION REQUIREMENTS

Distinctiveness authentication is mandatory to create sure the message transferred in the VANETs has a justifiable sender. Data reliability is essential to avoid the data to be tampered and damaged by a malicious node. Non- denial is apprehension to make certain the justifiable nodes which constantly forwards the message or is the source of the message denying their processing to the message. In our protocol, intermediary node in multi-hop communications requirements to modify the location information of the packets, so each nodes receive contribute in transit the packet necessitate be confident not repudiate their performance. Routing legality. The protocol necessity has the function to discover and bypass the malicious nodes to keep the routing running accurate.

IV. HYBRID AUTHENTICATION PROTOCOL

The system can be recapitulate into two characteristic Security approach for Routing message ,Approach for Node estimate intended for the security of the routing message, a signature established method is employed to realize end-to-end authentication and reliability of the data. And for the evaluation mechanism, every node is turned on hybrid authentication protocol and verifies every one packet send by its neighbor. The protocol estimate the steadfastness of neighbor nodes by inspection its forwarding ratio. A signature meadow is added to the packets of routing data. Excluding the IP header and the signature meadow, supplementary information is present to the location-based protocol. We get the signature as follows: Suppose with the intention of every node has an ID-based confidential key and a community key. Such as node n has a confidential key and can calculate a community key^{com} based-on ID of node m when node n needs to verify the packet receive from node m.

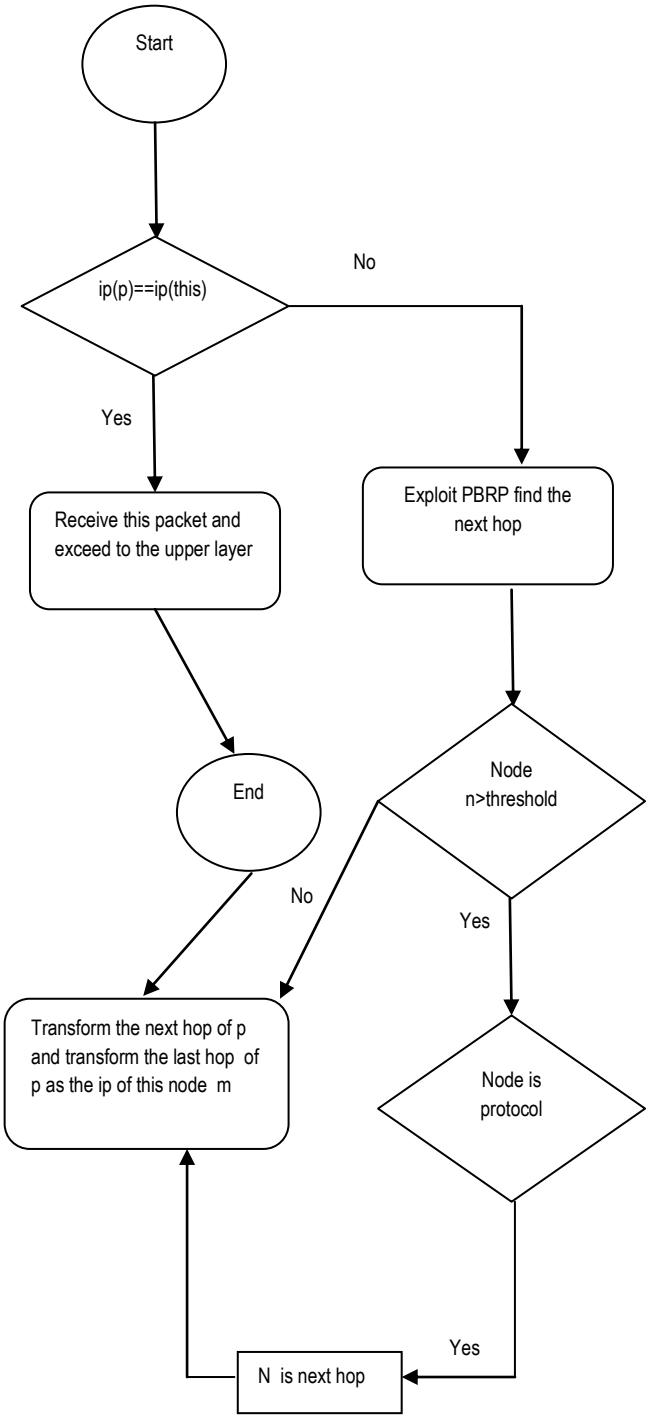
The packets sender node m gets the signature as (1). When one node receives a routing data packet, firstly, the packet will be verified and the equality (2) will be checked if it is true. The evaluation mechanism is divided into two aspects: forward estimation and backward estimation. Forward estimation is employed to find out the drop malicious nodes. The operational opinion of the forward estimation is as follows: Assuming that node n is the neighbor of node m, and taking an example that node m access node n to explain how forward estimation mechanism workings. When node m forwards or sends packets to node n, node m process the packet as approach 1 described.
Method: 1 of part I is how the node m records every exact packet to node n.

Method: I part II is applied in listening function. Another part of forward estimation, node m counts the packets of neighbor n normally send depending on it.

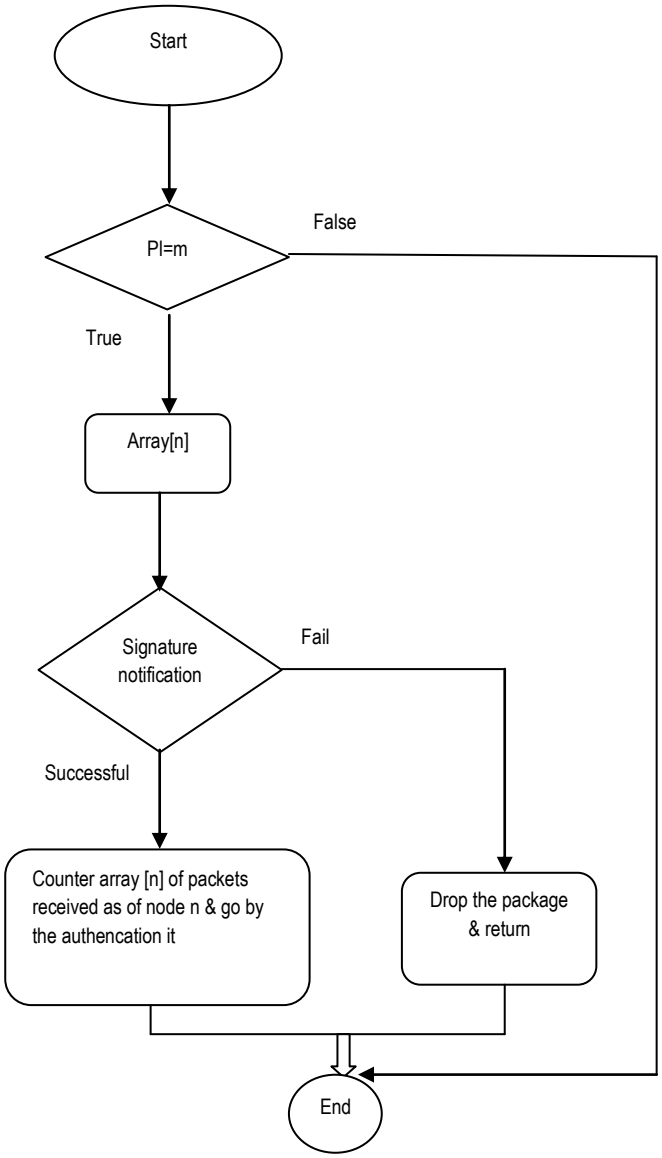
Method: 2 is to check if the packet p send by node n is received from node m. And then increases 1 on the counter which records the number of packets node n send normally.

Method: 3 is a part of a timer implementation is a part of a timer implementation in the protocol. This algorithm mainly used to calculate the evaluation value of every neighbor of node m. A certain time slot can be set to adjust the valuation frequency. is to figure out the forward estimation value based on the data record prior.

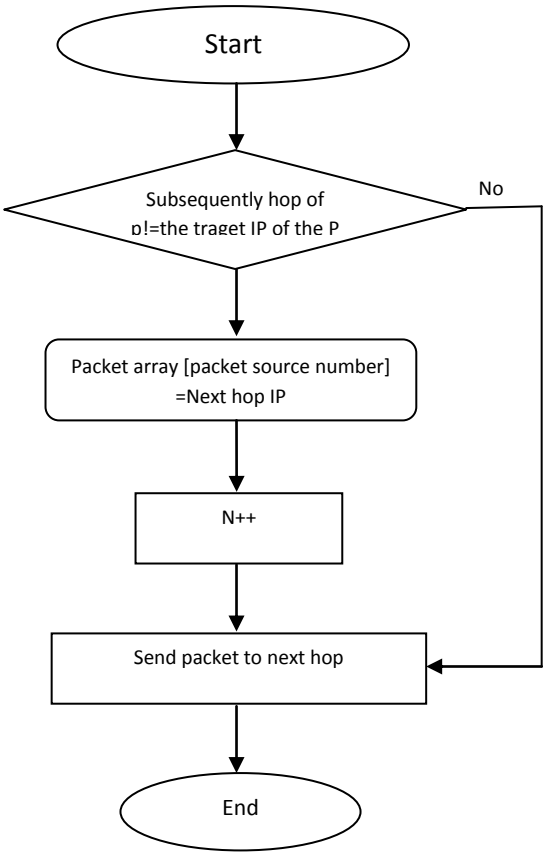
Method: I part I



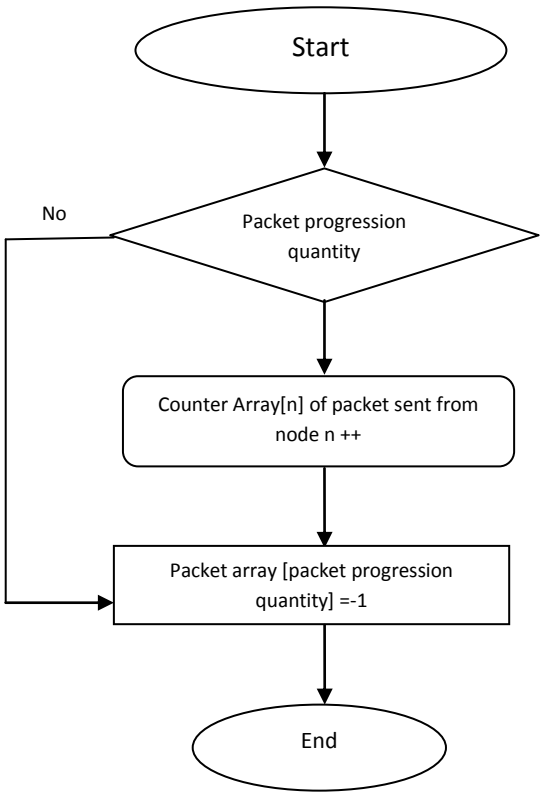
Method: I part II



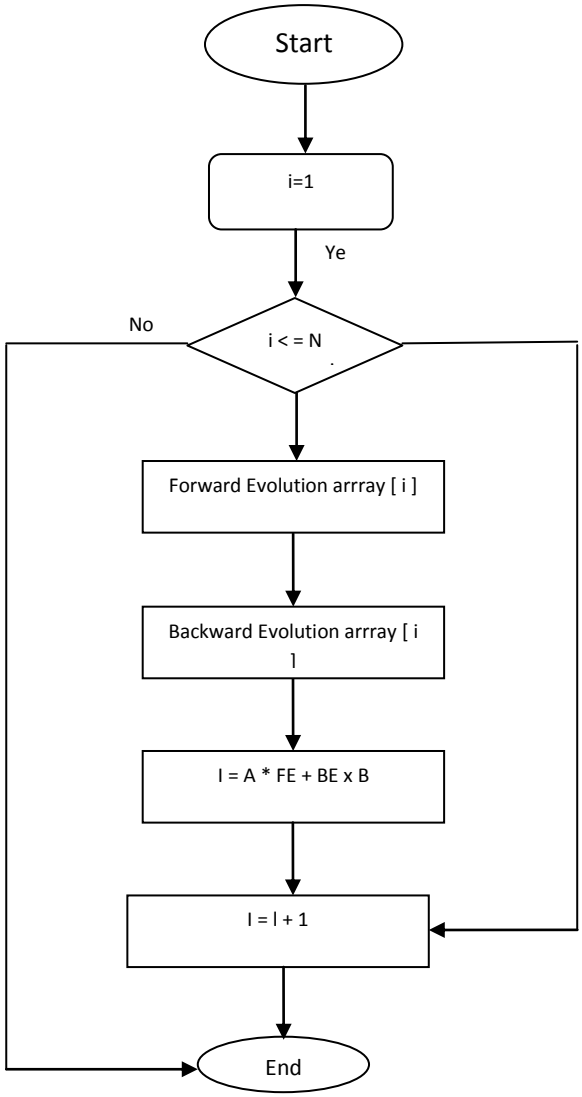
Method: I part III



Method: 2



Method: 3



V. CONCLUSIONS

A protection method for LBR protocol was proposed eading in this paper the most important idea of this method is the estimation mechanism. Meanwhile the solution combined the Hybrid Authentication Digital Signatures Certificates. Digital Signature functional to end to end, hope to hope to protect the routing messages from being tempered by malicious nodes, and assistant to backward evaluation mechanism

REFERENCES

[1] Subir Biswas, Jelena Miˇsi´c, Location-based Anonymous Authentication for Vehicular CommunicationsISPIMRC-2o11.

[2] Yu-Chih Wei, Yi-Ming Chen, Hwai-Ling Shan Beacon-based Trust Management for Location Privacy Enhancement VANETs. IEEE-2011.

[3] Debasis Giri and Durbadal Chattaraj. A Secure and Efficient Communication in VANET 978-1-4244-7585-8/10-IEEE 2010.

[4] M. Raya, P. Papadimitratos, and J.-P. Hubaux,Securing vehicular communications, Wireless Communications, IEEE, vol. 13, no. 5, pp. 8–15, October 2006.

[5] Y. Sun, R. Lu, X. Lin, X. S. Shen, and J. Su, An efficient pseudonymous authentication scheme with strong privacy preservation for vehicular communications,Vehicular Technology, IEEE Transactions on, vol. 59, no. 7, pp. 3589 –3603, 2010.

[6] Li He and Wen Tao Zhu, Mitigating DoS Attacks against Signature-Based Authentication in VANETs 978-1-4673-0089-6/12/IEEE-2012.

[7] X. Lin, X. Sun, P.-H. Ho, and X. Shen,―Gsis: A secure and privacypreserving protocol for vehicular communications, Vehicular Technology, IEEE Transactions on, vol. 56, no. 6, pp. 3442–3456, Nov. 2007.

[8] Q. Wu, J. Domingo-Ferrer, and U. Gonzalez-Nicolas, Balanced trustworthiness, safety, and privacy in vehicle-to-vehicle communications, Vehicular Technology, IEEE Transactions on, vol. 59, no. 2, pp. 559 –573, 2010.

[9] G. Calandriello, P. Papadimitratos, J. P. Hubaux, and A. Lioy, ―Efficient and robust pseudonymous authentication in VANET, in VANET ’07: Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks. ACM, 2007, pp. 19–28. [Online].Available:http://dx.doi.org/10.1145 /1287748.1287752.

[10] R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, ―Ecpp: Efficient conditional privacy preservation protocol for secure vehicular communications,‖ in INFOCOM. IEEE, 2008, pp. 1229–1237.

[11] S. D. Galbraith, K. G. Paterson, and N. P. Smart,―Pairings for cryptographers, Discrete Appl. Math., vol.156, pp. 3113– 3121, September 2008.[Online]. Available:http://portal.acm.org/citation.cfm?id=14503 45.1450543

[12] S. Biswas and J. V. Misic, ―Deploying proxy signature in vanets, in GLOBECOM. IEEE, 2010, pp. 1–6

[13] Nizar Alsharif, Albert Wasef, and Xuemin (Sherman) Shen, ESPR: Efficient Security Scheme for Position-Based Routing in Vehicular Ad Hoc Networks, GLOBECOM-IEEE Global Telecommunications Conference, Miami, December, 2010, pp. 1-5.

[14] Brad Karp, H. T. Kung, GPSR:Greedy Perimeter Stateless Routing for Wireless Networks