A Survey of Anonymous Authentication Schemes Based on Pmipv6 in Vehicular Ad HOC Networks

Dr. K. Suresh Babu[1], Thanugula Dhanunjay Varma[2]

[1]*Associate Professor of CSE, School of Information Technology, JNT University, Hyderabad, Telangana- 500 085*

[2]*M.Tech Scholar of CSE, School of Information Technology, JNT University, Hyderabad, Telangana- 500 085*

Abstract- Vehicular ad hoc network (VANET) can build the traffic proficiency by enabling arbitrary vehicles to communicate the messages to different vehicles and road side units (RSUs). Yet, because of the wireless of the remote system, VANET is truly helpless against forgery assault. To keep up consistent and ubiquitous Internet availability, a proficient handoff conspire must be utilized when portable users traverse distinctive access systems. In any case, in the urban vehicular condition, the high speed of vehicles and random mobility of users force incredible difficulties to the plan of a compelling handoff conspire. In this paper, we proposed and examined different routing protocols for VANET. The sorts of VANET frameworks specifically, Efficient PMIPv6 (E-PMIPv6), Privacy protection authentication scheme (PPAS), Diffie-Hellman Key based authentication scheme (DHKA), and Cooperative Quality-aware service access system (CQASA). This paper exhibits a Literature study of the calculations clarifying the ideas of unknown verification plans. Various routing algorithms have been examined by authors to enhance the security, productivity and decrease the signaling overhead.

Keywords- Urban vehicular networks, Proxy Mobile IPv6, Network mobility, PMIPv6, Authentication, Internet of vehicles, Quality-aware, Privacy protection, E-PMIPv6, PPAS, DHKA, and CQASA.

I. INTRODUCTION

The target of smart urban communities is to enhance the nature of a subject's life. In such manner, the transportation division is of incredible significance because of the quickly expanding number of vehicles in enormous urban areas, which makes traffic the board for smart urban areas rather difficult [1]. As a vehicular client driven system, the vehicular social network (VSN) profoundly incorporates informal communities and the Internet of Vehicles (IoVs). As of late, vehicular correspondence systems are at a turning point, with application targets changing from road traffic safety and transportation productivity to VSNs, which can give far reaching social administrations to residents. Different driving IT organizations are entering this territory. For example, Apple propelled the vehicle framework Carplay in March 2014, by which clients can take an interest in social exercises easily and securely. Google participated in the improvement of VSNs by discharging Andriod Auto in June 2014 [2].

With the quick improvement of remote correspondence innovations, there is an expanding number of traveling users to get to Internet through IP-empowered smart gadgets. They are anxious to appreciate nonstop and universal Internet sight and sound administrations, e.g., video gushing, web perusing, and file downloading, and so on., despite the fact that vehicles may wander crosswise over various access systems (e.g., WiFi, WiMAX, LTE/3G) in the urban transportation condition [3]– [5]. So as to meet differing Quality of Service (QoS) necessities of these mixed media administrations, vehicular systems need to help consistent remote interchanges with low handoff inertness, low packet loss, decreased flagging overhead, and so forth.

While, not quite the same as the expressway situation where versatile clients more often than not get remote network to Internet through settled RSUs, in the urban condition open transportation vehicles (e.g., city transport, metro train) might be equipped with MRs and furnish remote access to portable clients with smart gadgets. Thus, the complex client versatility in the urban condition typically instigates visit handoffs when portable clients travel starting with one access arrange then onto the next access organize (e.g., a portable client may get off an open transportation vehicle at a station and switch its remote association from a MR to a settled RSU), which enormously debases the correspondence execution. Thusly, a proficient versatility the executives conspire must be intended to help consistent handoff when portable clients cross distinctive access organizes, and enhance handoff execution by diminishing handoff idleness, parcel misfortune, and flagging overhead, and so forth., in every handoff situation [6].

Versatile IPv6 (MIPv6) [7] is a generally acknowledged standard to help worldwide portability for Mobile Hosts (MHs). The augmentations of MIPv6, for example, Fast-Handovers for Mobile IPv6 (FMIPv6) [8], Hierarchical MIPv6 (HMIPv6) [9], [10], Fast Handover for Hierarchical MIPv6 (FHMIPv6) [11], and so on. Have been institutionalized by Internet Engineering Task Force (IETF) to enhance handoff execution.

II. RELATED WORK

In [12], author proposed PMIPv6 relocates the portability usefulness residing in MHs to organize elements, and gives transparent versatility the board to MHs without changing their IP addresses. In any case, PMIPv6 experiences long handoff delay and high packet loss, and needs versatility support for NEMO.

In [13], author proposed to enhance PMIPv6 in IEEE 802.11 systems. The plan proposes to trade verification data and HNPs of MHs between neighboring passages, and decreases the aggregate handoff dormancy by dispensing with setting acquisition delay. In any case, despite everything it encounters overwhelming packet loss amid the handoff procedure.

In [14], author proposed to help quick handoff in vehicular systems. By using the Global Positioning Systems (GPS) arrange data and the development heading of a MH, the p-MAG can distinguish the correct n-MAG from its neighboring MAG table ahead of time, which abbreviates the handoff delay.

In [15] author proposes to accommodate NEMO in PMIPv6 to give straightforward handoff to a whole portable system in intelligent transportation frameworks. Also, as an augmentation to P-NEMO, FP-NEMO pre-builds up a bi-directional passage between the p-MAG and the n-MAG to trade downlink or uplink bundles amid the handoff procedure, which effectively decreases packet loss. Be that as it may, P-NEMO and FP-NEMO just help NEMO for a versatile system.

In [16], author proposed an upgraded quick handover conspire EfNEMO is proposed for NEMO, and a MR leads a provisional restricting refresh to enlist another CoA before the Layer-2 (L2) handoff. Accordingly, packets bound to MHs are sent through the way between the HA and the n-MAG, and packet burrowing between the p-MAG and the n-MAG is wiped out.

III. EFFICIENT PROXY MOBILE IPV6 BASEDHANDOFF SCHEME

Y Bi, H Zhou, W Xu, X Shen, H Zhao [6], author propose an upgraded PMIPv6 based handoff scheme E-PMIPv6 to give consistent and straightforward portability management to MHs in urban vehicular systems. In the underlying registration process, E-PMIPv6 empowers individual MHs to get availability from either settled MAGs or MRs, and supports Home Network Prefix (HNP) portions for a gathering of MHs inside a similar versatile system that just possesses one BCE at the LMA, which is not quite the same as existing plans where each MH involves a different BCE at the LMA, and altogether enhances buffer resource utilization. In the handoff procedure, E-PMIPv6 completely considers four handoff situations to give straightforward portability support to MHs wandering crosswise over different access systems, and adaptably uses packet buffering and tunneling instruments in every handoff situation, which decreases handoff delay and prevents packet loss.Accordingly, the contributions of this paper [6] are summarizedas follows.

1) E-PMIPv6 productively uses cache assets at the LMA by consolidating the BCEs of MHs inside a similar versatile system in the urban transportation framework, where the LMA is as a rule accountable for portability the executives for a huge number of MHs.

) E-PMIPv6 mutually considers diverse handoff situations by giving proficient portability support to MHs when they roam crosswise over various access arranges in the urban vehicular condition (e.g., from a settled RSU to another RSU, from a MR to another MR, or between a settled RSU and a MR), and enhances handoff execution by eliminating packet loss, diminishing handoff latency and signaling overhead, and so on., in every handoff situation.

3) We present an itemized logical model to examine the execution of E-PMIPv6 regarding handoff idleness, signaling overhead, buffering cost, and tunneling cost, and so on., and approve the diagnostic outcomes by broad simulations.

In E-PMIPv6, so as to set up a conclusion to-end association with the CN, a MH or MR needs to direct the underlying restricting enrollment to acquire HNPs from an entrance system, and afterward it can design its IP address and access Internet administrations. In any case, when it goes from the present access system to another one (e.g., from a MAG to another MAG, from a MR to another MR, or between a MAG and a MR) in the urban condition, it needs to lead one of the four handoffs presented.

A. Initial Binding Registration

At the point when a MR empowered vehicle moves into the E-PMIPv6 space, the MR at first sends a Router Solicitation (RS) message to the appended MAG to request HNPs for VMNs and FMNNs in the MR empowered vehicle. On accepting the RS message, the MAG makes a Binding Update List Entry (BULE) to keep the enlistment data for the MR. At that point, it instates an enrollment Proxy Binding Update (PBU) message, and conveys it to the LMA. So as to conform to PMIPv6, E-PMIPv6 needs to allot a HNP to each VMN or FMNN that is appended to the MR. Consequently, the altered RS message is reached out to convey the quantity of asked for prefixes.

B. Handoff Process

The handoff procedure is activated when a MR or MH is moving out of its present access organize. For instance, a VMN may encounter any of the four handoff situations, a MR/VMN/FMN needs to direct the MAG-MAG handoff when they roam crosswise over various MAGs, yet a FMNN isn't required to lead handoff since it for all time appends to a settled MR on the vehicle.

IV. PRIVACY PROTECTION AUTHENTICATION SCHEME

Hui Zhu, Tingting Liu, Guanghui, and Hui Li [17], author propose a validation plot PPAS dependent on the highlights of the bilinear pairing and the elliptic curve. PPAS can give compelling assurance of protection and obscurity among vehicles and foundations. The proposed plan PPAS incorporates three stages: System Setup, Membership Registration, and Authentication.

So as to secure VANETs, the accompanying security necessities ought to be fulfilled by PPAS [17] plot.

(1) Message integrity and verification. Message honesty is required to guarantee that the substance of the got information is neither adjusted nor replayed. What's more, substance validation is likewise a concern to guarantee that the communicating elements including vehicles, CC and RCs are genuine.

(2) Identity security saving. The genuine character of a vehicle ought to be kept unknown from different vehicles, RSUs, and RCs. In another word, character security saving is fundamentally identified with averting disclosure of a vehicle's genuine personality by observing and breaking down the correspondence in a VANET.

(3) Traceability and revocability: Traceability is required to acquire a vehicle's genuine personality by CC. Also, revocability is used to deny any acting up element from the system to ensure the wellbeing of other authentic elements in VANET.

i. System setup

The procedure of framework setup is determined as pursues. This progression will be executed once for the entire framework under ordinary conditions, except if the protection key of CC is under doubt of being endangered, or CC means to improve the security dimension of the framework through refreshing the parameters and the security key occasionally.

ii. Membership registration

As like the framework setup, this progression ought to be executed just once except if the genuine character of a vehicle is distinguished to be compromised.

iii. Local authentication

At the point when the client Vehicle-i moves into its enrollment region, the validation procedure will be spoken to in message character criteria.

➢ Security analysis

In this situation, we use the unauthenticated-joins adversarial model (UM) in Canetti-Krawczyk (CK) demonstrate which was proposed by Bellare, Canetti and Krawczyk.

The adversary in the model endeavors to break the convention by associating with the substances, and two adversary models are characterized: the confirmed connections adversarial model (AM) and UM. In the AM, the foe is confined to conveying messages steadfastly; while in the UM, the foe cannot just control correspondence joins and the planning of activity occasions, yet in addition the private data in the member's memory through express assaults.

V. Diffie-Hellman Key based authentication scheme

Hyungon Kim, Jong-Hyouk Lee [18], author present a Diffie-Hellman (DH) key based confirmation scheme that uses the low layer signaling to trade DH factors and permits versatility benefit provisioning elements to trade portable hub's profile and continuous sessions safely. All the more absolutely, the presented DH key based confirmation conspire has the accompanying unmistakable highlights contrasted with PMIPv6.

- DH key trade activity is received to decrease the calculation overhead.
- Relevant portability benefit provisioning substances are upheld to play out the setting exchange and information packet sending.
- Pre-built up security relationship between portability benefit provisioning substances are not required.

By using the particular highlights, the DH key based validation conspire accomplishes low handover latency while giving secure handover administration to MNs in PMIPv6. The present particulars of PMIPv6 and FMIPv6 just give the convention tasks without secure confirmation concerns.

As needs be, the proposed DH key based confirmation plan would be a decent direction for secure verification for PMIPv6.

A. Diffie-hellman key based authentication

The followings are the structure standards and suspicions of the DH key based verification scheme.

- Minimizing the calculation power utilization and the managerial cost forced on the MN.
- Minimizing the quantity of keying material solicitations to the AAAh (AAA home server).
- Utilizing signaling messages characterized in FPMIPv6 to enhance handover execution.
- Utilizing L2 events to anticipate the handover of the MN.
- Utilizing L2 messages so as to convey DH factors.
- Protecting session keys against different assaults.
- Removing pre-set up security relationship between the MAGs.
- Removing extra signaling messages between the MAG and the LMA.

One of ongoing execution upgrade approaches is to utilize interface layer explicit data. For example, IEEE 802.21 (MIH)

gives connect layer explicit data to upper layers. Particularly, some data given by IEEE 802.21, for example, accessible system list, link identification, interface status, and so on, can be utilized to encourage the handover decision and recognition of the MN. In this paper, we expect that the MN and system elements know about MIH functionalities.

B. Security analysis

The proposed plan reuses the recently assigned session keys to accomplish low handover latency. However, security shortcomings about this key reuse must be tended to. In like manner, we bring up a conceivable session-taking assault on the proposed plan. So as to re-utilize the session keys, in any case, they must be assumed control in a safe design between the significant MAGs (mobile access gateway).

VI. Cooperative Quality-Aware Access Service Selection Scheme

Zhaolong Ning, Xiping Hu, Zhikui Chen, and Mengchu Zhou [19], authors structures a Cooperative Quality-aware Service access (CQS) framework for SIoVs. Its primary commitment can be outlined as pursues:

1. We set forward a dynamic access service evaluation scheme. It completely considers the direct and indirect administration quality assessments, and can adapt to the obstruction and impact brought by the dynamic difference in system topology and node instability by presenting a period property, attenuation mechanism, and criticism direction component of the historical record.
2. We propose a social relationship development strategy for intelligent vehicles. In light of the establishment of occupation likeness and social relationship in SIoVs, we set up a sensible and adaptable social relationship show by investigating the certain interior similarity inside vehicles to advance the precision and achievement rate of an administration get to strategy.
3. We propose a forecast strategy as indicated by vehicle development direction for collaboration time estimation. By breaking down the development rate and traits of vehicles, their development direction can be anticipated, and the variety propensity can be determined for the reference of moving vehicles.
4. We develop a CQS framework for SIoVs. At initial, a node-centric generation tree is utilized to assess the access quality. At that point, distinctive access benefit routing selection techniques are utilized to choose the entrance way as per the present system state. From that point onward, a bi-heading buffering calculation is given to advance the reaction effectiveness and precision of directing. Execution assessments show that, contrasting and the current plans, our CQS plan can build the normal administration quality, number of packets sent per access and system achievement rate by around 25%, 20% and 5%, individually.

A. Quality-Aware Access Service Selection Scheme

As appeared in Fig. 1, we consider a heterogeneous and decentralized system situation, where no fixed trust expert exists to give trust assessment. Node hardware moves with clients, and joins or leaves the system progressively. Every gadget contains its own data, for example, the interest and gave benefit. Client interest speaks to the characters and focal points of the gave administration, which can be seen as a guide between client social association in reality and the social relationship among gadgets in the system framework.

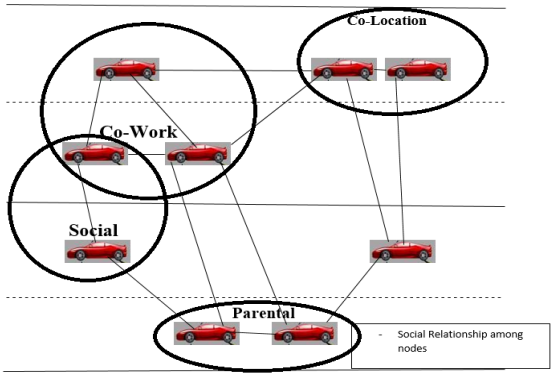

Fig.1: System model

B. Cooperative Quality-Aware Service Access

Since connection associations are unsteady in SIoVs, a system structure fluctuates after some time and impedance conditions are complex. In this manner, how to choose an appropriate access article and transmission interface is a critical issue. Unfortunately, it is hard to enhance the choice of both access node and transmission interface. In this segment, by completely considering system access from the perspective of both system hubs and connections, we present the CQS strategy.

C. Network model

As per the proposed plan, nodes can perceive and assess different gadgets from the aspects of access QoS, node social relationship and association time forecast, in light of which get to demand can be propelled by reasonable gadgets. In SIoVs, since nodes speak with one another by remote advances, (for example, Bluetooth and WiMAX), correspondence among gadgets is confined by the spread way. So as to successfully recognize arrange benefit with a bigger range, we further broaden the QoS-mindful access benefit choice plan to multi-jump dynamic system condition.

With the goal of collaborating with different gadgets outside their correspondence extend, a neighborhood dataset, including access benefit record and arrangement data, is utilized to assess benefit quality and investigate node social relationship. Moreover, the data of directing, buffer, and

neighbor ought to likewise be kept up by node gadgets. Details are represented underneath.

As per the assumed job amid the procedure of system get to, bode gadgets can be commonly characterized into: 1) Service requester, i.e., the node that dispatches an administration get to ask for; 2) Service supplier, including gadgets that can give administrations to other people; 3) Service colleague, i.e., the node that gives the administration of system access or course. It is noticed that the job of any node gadget may change or assume various jobs. A node gets packets from its encompassing nodes periodically, and performs directing as per their sorts. Amid each cycle, a node additionally communicates its design and neighbor data, and sends packets for an administration ask for if essential.

The fundamental considerations are:

a) From the part of QoS, long routing separation goes with high interference hazard because of the low stability in vehicular systems. Be that as it may, the correspondence separate breaking points organize QoS of the crossing tree.

b) From the thought of system cost and computational cost, a bigger spanning tree requires more reference points for support. Furthermore, it is additionally asset devouring for nodes to register and keep up a neighbor arrange crossing tree. A node first checks its received queue, and confirms whether a got packet is redundant. Provided that this is true, the node makes a decision about whether a progressively solid routing path exists as indicated by the recognition consequence of the entrance QoS, and decides if to refresh its directing table or not.

VII. Comparison of authentication schemes in vehicular ad hoc networks

S.NO.	Author	Title	Analysis
1.	Y Bi, H Zhou, W Xu, X Shen, and H Zhao	An Efficient PMIPv6-Based Handoff Scheme for Urban Vehicular Networks	Low packet loss, Signaling overhead, Decreasing buffering cost
2.	Hui Zhu, Tingting Liu, Guanghui, and Hui Li	PPAS: privacy protection authentication scheme for VANET	Security more, Communication overhead decreases, authentication more
3.	Hyungon Kim, Jong-Hyouk Lee	Diffie-Hellman key based authentication in proxy mobile IPv6	Minimizes authentication latency, improve the scalability, probability more
4.	Zhaolong Ning, Xiping Hu, Zhikui Chen, and Mengchu Zhou	A Cooperative Quality-aware Service Access System for Social Internet of Vehicles	Reliability, quality of service more, average request cost over its peers, and improve the efficiency

VIII. CONCLUSION

This paper presents a detailed literature of the most recent best in class routing strategies in VANETs. The idea of sensor nodes and cluster head distinguishing proof is depicted in detail. This procedure is trailed by the verification conspires and give the security in directing dimensions. We exhibited the convention task and security examination of the proposed plan. The numerical outcomes confirm that the different proposed plans decreases the handover verification idleness and it outperforms regarding handover latency, security, and routing overhead.

IX. REFERENCES

[1]. DorinaPojani, Dominic Stead, “Sustainable Urban Transport in the Developing World: Beyond Megacities”, Sustainability, 2015.

[2]. Zhaolong Ning, Feng Xia, Noor Ullah, Xiangjie Kong, and Xiping Hu, “Vehicular Social Networks: EnblingSmart Mobility”, IEEE Communication Magazine, April, 2017.

[3]. H. Luan, X. Ling, and X. Shen, “Provisioning QoS controlled mediaaccess in vehicular to infrastructure communications,” *Ad Hoc Netw.*,vol. 10, no. 2, pp. 231–242, Jul. 2010.

[4]. H. Zhou *et al.*, “Spatial coordinated medium sharing: Optimal accesscontrol management in drive-thru Internet,” *IEEE Trans. Intell. Transp.Syst.*, vol. 16, no. 5, pp. 2673–2686, Oct. 2015.

[5]. X. Liu and W. Zhuang, “MCIP: A 3G/IP interworking system supportinginter-cluster soft handoff,” *Wireless Pers. Commun.*, vol. 39, no. 3,pp. 279–305, Nov. 2006.

[6]. Y Bi, H Zhou, W Xu, X Shen, H Zhao, "An Efficient PMIPv6-BasedHandoff Scheme for Urban Vehicular Networks," IEEE Transactions onIntelligent Transportation Systems, vol.17, no.12, PP.3613-3628, Dec.2016.

[7]. D. Johnson, C. Perkins, and J. Arkko, “Mobility support in IPv6,” InternetEng. Task Force, Fremont, CA, USA, RFC 3775, Jun. 2004.

[8]. R. Koodli, “Mobile IPv6 fast handovers,” Internet Eng. Task Force,Fremont, CA, USA, RFC 5568, Jul. 2009.

[9]. H. Soliman, C. Castelluccia, K. ElMalki, and L. Bellier, “HierarchicalMobile IPv6 (HMIPv6) mobility management,” Internet Eng. Task Force,Fremont, CA, USA, RFC 5380, Oct. 2008.

[10]. S. Pack, T. Kwon, Y. Choi, and E. K. Paik, “An adaptive network mobilitysupport protocol in hierarchical mobile IPv6

networks," *IEEE Trans. Veh.Technol.*, vol. 58, no. 7, pp. 3627–3639, Sep. 2009.

[11]. H. Y. Jung, H. Soliman, S. J. Koh, and N. Takamiya, "Fast handover forhierarchical MIPv6 (FHMIPv6)," Internet Eng. Task Force, Fremont, CA,USA, IETF draft, draftjungmipshopfhmipv600.txt, Oct. 2005.

[12]. V. Sandonis, M. Calderon, I. Soto, and C. J. Bernardos, "Design andperformance evaluation of a PMIPv6 solution for geonetworking-basedVANETs," *Ad Hoc Netw.*, vol. 11, no. 7, pp. 2069–2082, Sep. 2013.

[13]. J. C. Lee and D. Kaspar, "PMIPv6 Fast Handover for PMIPv6 Based on802.11 Networks," Network Working Group, Internet Eng. Task Force,Fremont, CA, USA, Jan. 2007.

[14]. A. Moravejosharieh and H. Modares, "A proxy MIPv6 handover schemefor vehicular ad-hoc networks," *Wireless Pers. Commun.*, vol. 75, no. 1,pp. 609–626, Mar. 2014.

[15]. J. H. Lee, T. Ernst, and N. Chilamkurti, "Performance analysis ofPMIPv6-based NEtworkMObility for intelligent transportation systems,"*IEEE Trans. Veh. Technol.*, vol. 61, no. 1, pp. 74–85, Jan. 2012.

[16]. S. Ryu, K. J. Park, and J. W. Choi, "Enhanced fast handover for networkmobility in intelligent transportation systems," *IEEE Trans. Veh. Technol.*,vol. 63, no. 1, pp. 357–371, Jan. 2014.

[17]. Zhu, H., Liu, T., Wei, G. et al., "PPAS: Privacy protection authentication scheme for VANET", Cluster Comput (2013) 16: 873.

[18]. Kim H, Lee J H, "Diffie-Hellman key based authentication in proxy mobile IPv6," Mobile Information Systems, Vol.6, no.1, pp.107-121, Jan. 2010.

[19]. Z. Ning, X. Hu, Z. Chen, M. Zhou, B. Hu, J. Cheng M. Obaidat, "A Cooperative Quality aware Service Access System for Social Internet of Vehicles,"IEEE Internet of Things Journal, Doi: 10.1109/JIOT.2017.2764259,2017.