

security in the VANET such as cryptographic schemes reputation-based systems, and plausibility and sensor-driven techniques.

VSPN: VANET-Based Secure and Privacy-Preserving Navigation

The author in [1] has proposed compute real time road traffic through VSPN protocol. In this system it uses Road side unit (RSU) and Trusted Authority (TA) and on board unit to give real time road traffic. In this system OBU continually communicate with RSU and TA, OBU request for the navigation to RSU, RSU check whether destination is in within his ranger or not and also same time check traffic in that region. if destination is not in current RSU range then it broadcast navigation message to all nearby RSU. This protocol provides security from message integrity and authentication, Identity privacy preserving, traceability and confidentiality. It uses bilinear mapping to map secrete key to public key mapping, and uses Boneh–Lynn–Shacham (BLS) signature scheme [12] to provide security from message forging.

Inter node Mobility Correlation for Group Detection and Analysis in VANET, [3] has proposed mobility correlation among the moving vehicle. In VANET network devices communicate with RSU unit through wireless network which leads to connection and disconnection of communication link and network and grouping and dispersion of nodes, which greatly affect the network performance. at the same they also form a group of vehicle which ave similar pattern of movement. To measure correlation among vehicle he uses spatial locality node [SLS] mobility and temporal locality of node pattern [TLS]. And after calculating both values of SLS and TLS he introduces third technique which is dual locality reference [DLR]. Vehicular Security through Reputation and Plausibility Checks [2] uses user's reputation and plausibility to perform security in the VANET network. This technique provides security against data modification, wrong event generation and data collection and data falling. In this protocol faulty nodes identify and remove it from the network. This algorithm mainly targeted on information which transfer on the network it may by single hop or multi-hop network. Efficient Conditional Privacy Preservation Protocol In this proposed system [5] provides two solutions, on anonymous authentication for safety messages with traceability of node who originated the message. The architecture in this method contains Trusted Authority [TA] or main server who constantly communicate with Road Side Unit [RSU], RSU communicate with on board Unit [OBU] to direct location of the message. The OBUs are constantly communicate with the running vehicles and broadcast real traffic information to themselves and also others who request the key. TA: Ta is responsible for registration of RSU and

OBU and give key to them. The RSU which can communicate with both OBU and TA has storage capacity. It can tell give message to the user about real time road traffic so user can adjust his route.

Secure Vehicular Communications Systems: Design and Architecture. The authors in [4] have proposed a secure architecture. The architecture consists of the certification authority (CA) where each authority is responsible for assign block or territory. Each authority provides certificates to nodes which are in his territory and also accept nodes out of his nodes which have other certification authority's key nodes enter its territorial boundary. The RSU and on board Unit store the vehicle private key when they enter the other CA's boundary for the signature purpose. It is used as a tamper resistant solution to prevent against physical on-board tampering. Every node utilize high number of public private key for short duration of time (called pseudonyms that hide the real user of the node) instead of just using one public - private key for long term which will easy to crack for attacker. Every node uses a pseudonym for a minimum period of time and then change to next identity. This provides the required privacy Secure Positioning Based Routing (PBR) for VANETs. This protocol [16] depends on asymmetric cryptography and digital signatures. When there is only one node that is transferring the packet then it has to sign in that packet before it can send to the destination. If it dealing with more than one hop then two way signature on the packet is proposed, source signature and sender Signature, in this way we can protect data from modification. When packet reach to the destination it has perform number of checks for packets integrity. In order to check when message is originated time stamp is added with the message. This timestamp is important to check time window of the message. Additional restrictions are added by assuming a peak sending scope of the nodes in the network. Speed of the message is also calculated by time difference between two neighboring nodes and multiplying it with highest speed of the nodes. This protocol set maximum message a node can send so it will restrict malicious nodes to broadcast false message in to the network. If any node is sending more messages than its limit then this protocol will block this node from message transferring. In[13] different groups are formed deepening their geographical location and groups pass messages to the each other. In this method group leader is selected randomly and through group leader messages are passed. In this except group leader all nodes are safe from external attacks only group leader security is in danger. In [19] use hybrid technique to give user real time road traffic to the user. in this method it use both VANET and MANET technologies to give real time road traffic. It proposed real time path planning algorithm to reduce average traveling cost by avoiding vehicle getting stuck in the traffic. It improves overall performance of the VANT network by giving real time road traffic information.

Table 2: summery of literature survey

<i>Sr. No</i>	<i>Paper Name</i>	<i>Methods</i>
1	Securing vehicular ad hoc networks, 2006.[16]	Certificate authority (CA) responsible particular region. Each node use short term public private key called pseudonym. Keys revocation function performs by CA.
2	Inter node Mobility Correlation for Group Detection and Analysis in VANET, 2013.	Vehicle groups are formed on the basis of spatial Locality system and temporal Locality system. Combine feature of the system in Dual Locality system[DLS]
3	Vehicular Security Through Reputation and Plausibility Checks, 2007	Vehicle security is achieved by reputation and plausibility is check. Provides security against data modification dual signature sender and receiver checking.
4	ECPP: Efficient condition privacy preservation protocol for secure vehicular communication, 2008	Provides effective communication and location of the vehicle. It can provide real identity of the user at any time.
5	Securing cooperative data downloading in vehicle ad hic network.2013	Develop application layer protocol to share data between vehicles. It is reliable method to share data because after receiving data it also send acknowledgement.
6.	Security without Identification: Transaction Systems to Make Big Brother Obsolete, Comm. 1985	Take navigation credential from one organization and show to other organization. The two separate organizations are not linkable by this anonymous credentials achieved.
7.	An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks, Proc. 2008	Batch verification scheme is known as IBV introduce for verification of large number of RSU. The scheme relies on a temper-proof device to store an unchangeable master secrete key.
8.	A Next-hop Selection Scheme for Emergency Message Propagation in VANETs 2014	Nearest hop is selected when any emergency message has to broadcast. Message is divided in two parts according to their distance from the emergency location spot.
9.	AMOEBAs: [13] Robust location privacy scheme for VANET, 2007.	Groups are formed and group leader choose randomly in each group. By group leader all messages and data are transfer..

4. Conclusion

VANET is important technology in vehicle traffic management. It can give safety message to the other vehicle so millions of human life can be saved. To use VANET in daily day to day life, there are different protocols are available, which can provide security to this technology. Different protocols are available to address the security issues, all protocols have their advantage and disadvantage which can handle security related problems. These protocols provide security against above mention security threats.

References

- [1] VSPN: VANET-Based Secure and Privacy-Preserving Navigation T.W. Chim, S.M. Yiu, Lucas C.K. Hui, Senior Member, IEEE, and Victor O.K. Li, Fellow, IEEE IEEE TRANSACTIONS ON COMPUTERS, VOL. 63, NO. 2, FEBRUARY 2014
- [2] Sanjay K. dhurander, Mohammad Obaidat, Amrit Jaiswal, Akasaha Tiwari and Ankur Tyagi "Vehicular Security Through Reputation andPlausibility Checks" june 2014.
- [3] Yujin Li, Ming Zhao, Wenye Wang, Internode Mobility Correlation for GroupDetection and Analysis in VANETs IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 62, NO. 9, NOVEMBER 2013.
- [4] A. Studer, E. Shi, F. Bai, and A. Perrig, "Tacking Together Efficient Authentication, Revocation, and Privacy in VANETs," Proc. IEEE Sixth Ann. Comm. Soc. Conf. Sensor, Mesh and Ad Hoc Comm. and Networks (SECON), pp. 1-9, June 2009.
- [5] R. Lu, X. Lin, H. Zhu, P. H. Ho, and X. Shen, "ECPP: Efficient condition privacy preservation protocol for secure vehicular communi- cation," in Proc. IEEE 27th Conf. Comput. Commun., Apr. 2008.
- [6] B.K. Chaurasia, S. Verma, and S.M. Bhasker, "Message Broadcast in VANETs Using Group Signature," Proc. IEEE Fourth Int'l Conf. Wireless Comm. Sensor Networks (WCSN '09) Dec. 2008

- [7] C. Zhang, R. Lu, X. Lin, P.H. Ho, and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," Proc. IEEE INFOCOM '08, pp. 816-824, Apr. 2008
- [8] M. Raya and J. P. Hubaux, "Securing vehicular ad hoc networks," J. Comput. Security, vol. 15, no. 1, pp. 39-68, 2007.
- [9] T.W. F. Wang, D. Zeng, and L. Yang, "Smart Cars on Smart Roads: An IEEE Intelligent Transportation Systems Society Update," IEEE Pervasive Computing, vol. 5, no. 4, pp. 68-69, Oct.-Dec. 2006.
- [10] E. Fonseca and A. Festag, "A survey of existing approaches for secure ad hoc routing and their applicability to VANETs," NEC Network Laboratories, Heidelberg, Germany, NEC Tech. Rep. NLE-PR-2006-19, Version 1.1, Mar. 2006
- [11] G. Philippe, G. Dan, and S. Jessica, "Detecting and correcting malicious data in VANETs," in Proc. 1st ACM Int. Workshop Veh. Ad Hoc Netw., 2004.
- [12] D. Boneh, B. Lynn, and H. Shacham, "Short Signatures from the Weil Pairing," Proc. Seventh Int'l Conf. Theory and Application Cryptology and Information Security: Advances in Cryptology (ASIACRYPT '01), 2001.
- [13] A. Menezes, "An Introduction to Pairing-Based Cryptography," Math. Subject Classification, Primary 94A60, 1991
- [14] D. Chaum, "Security without Identification: Transaction Systems to Make Big Brother Obsolete," Comm. ACM, vol. 28, pp. 1030-1044, 1985.
- [15] Global Positioning System Standard Positioning Service Signal Specification. Navtech GPS Supply, 1995.
- [16] Secure Position-Based Routing for VANETs Charles Harsch, Andreas Festag¹, Panos Papadimitratos NEC Deutschland GmbH, ² EPFL, Switzerland, {charles.harsch|panos.papadimitratos}@epfl.ch
- [17] K. Sampigethaya, M. Li, L. Huang, and R. Poovendran, AMOEBA: Robust Location Privacy Scheme for VANET," IEEE J. Selected Areas in Comm., vol. 25, no. 8, pp. 1569-1589, Oct. 2007.
- [18] Secure Cooperative Data Downloading in Vehicular Ad Hoc Networks Yong Hao, Jin Tang, Member, IEEE, and Yu Cheng IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS/SUPPLEMENT, VOL. 31, NO. 9, SEPTEMBER 2013.
- [19] Real-Time Path Planning Based on Hybrid-VANET-Enhanced Transportation System Miao Wang_, Hanguan Shany, Rongxing Luz, Ran Zhang_, Xuemin (Sherman) Shen_, Fan Baix 2013