Detecting Sybil Attack with a Scalable Protocol

T. Hemalatha
New Prince Shri Bhavani college of Engineering and Technology, Gowrivakkam, Tamilnadu. India
E-mail: hemalathat90@gmail.com

Abstract - Vehicular ad hoc networks (VANETs) are being increasingly advocated for traffic control. Security and privacy are two major concerns in VANETs. Unfortunately, in VANETs, most of the privacy-preserving methods are vulnerable to Sybil attacks, whereby a malicious user can act as if to be multiple (other) vehicles. To ensure the authenticity of the messages propagated in VANET, a straight-forward process is to use public keys authorized by a certification authority (CA) to sign the messages. The certified public keys are called "pseudonyms". On the other hand, in order to prevent vehicles from being tracked by categorizing the keys that are utilized, each vehicle can switch between multiple pseudonyms, which are difficult to correlate to each other.

Keywords - Vehicular ad hoc networks (VANETs), privacy-preserving schemes, Sybil attacks, certification authority, and pseudonyms.

1. Introduction

Vehicular ad hoc networks (VANETs) are being increasingly advocated for accident avoidance, traffic control, and management of parking lots and public areas. Security and privacy are two major concerns in VANETs. Unfortunately, in VANETs, most of the privacy-preserving schemes are vulnerable to Sybil attacks, whereby a malicious user can pretend to be multiple (other) vehicles. For example [1], cars can collectively sense information about traffic congestion and relay them to other cars, toll stations, or the Department of Motor Vehicle (DMV) to facilitate traffic re-routing. Several other applications can become feasible if vehicles cooperate among themselves to achieve a common goal. When designing a cooperation-based system, it is important to address privacy and security concerns. The system requires being robust to non-cooperating entities, and should ideally be able to detect/punish them quickly. To ensure the authenticity of messages broadcasted in VANET, a straight-forward technique is to use public keys authorized by a certification authority (CA) to sign the messages [2]. The certified public keys are called pseudonym. Each vehicle can switch between multiple pseudonyms, which are difficult to correlate to each other. Among this approach, it is difficult for an attacker to identify vehicles by investigative the used keys.

These methods protects the privacy of the vehicles, it leaves another security hole. Because it is difficult to inform whether two messages are from the similar vehicle by investigative their public keys, a malicious vehicle may pretend to be many vehicles, and then distribute false information it is called Sybil attack. The harmful results of such attacks can cascade during the network. Vehicles are guessed to obtain a new pseudonym from a trusted Road-Side Box immediately before the earlier pseudonym expires. In [3] and [4], a light-weight solution is planned to resolve this problem. Vehicles simply hold one valid pseudonym at a moment, and are guessed to obtain a new pseudonym from a trusted Road-Side Box (RSB) or beginning the online CA if the present pseudonym becomes invalid. In this method, it is

critical that the vehicles have access to a CA when it requires updating its pseudonym. Without such an online environment support, the vehicles are not able to obtain new pseudonyms and send signed messages. Furthermore, if an attacker compromises an RSB, it can issue many certified pseudonyms to malicious vehicles, thus creating false messages in that area.

We propose a privacy-preserving scheme to detect the Sybil attacks in VANETs. The RSB is securely connected to the DMV via a backhaul wired network Our scheme the DMV to give vehicles with a lake of pseudonyms that are used for hiding the vehicle's unique identity. To prevent a vehicle from using multiple pseudonyms to direct a Sybil attack, the pseudonyms is assigned to a particular vehicle are hashed to a common value (One Way Hash Function).

We propose the Complete Two-Stage P2DAP Scheme, abbreviated as C-P2DAP. In P2DAP scheme, we delegate most of the detection to RSBs, and involve the DMV only when suspected vehicles need to be confirmed as a Sybil attacker. However, since RSBs are not trusted entities, the vehicle information available to the DMV cannot be transferred to the RSBs. In view of these constraints, we divide the vehicles into groups, and release the group information to RSBs. Such information allows RSBs to detect suspicious behaviour, but is not sufficient for RSBs to track vehicles, because RSBs cannot distinguish a vehicle from a group of vehicles. To group the vehicles, we use the one-way hash function to hash the pseudonyms during initialization.

The DMV knows the total amount of vehicles, and consecutively generates a sufficient amount of yearly pseudonyms for all the vehicles. After generating a pseudonym p, the DMV first hashes using a one-way hash function, everywhere κc is a global key. It chooses a set of bits from the hashed result to create hash collisions. The particular bits are referred as "coarse-grained hash value". The pseudonym p is located into a group, which stores the pseudonyms through the same coarse-grained hash values. The key κc will be distributed to all the RSBs. Next, the DMV calculates the hash value used for the above p through a new key κf, and chooses a set of bits from the result. The bits particular from the new hash value are referred as the "fine-grained hash value". The pseudonym p is located into a subgroup of the coarse-grained group, called fine grained group, in which all the pseudonym have the same fine-grained hash value.

2. Literature Work

According to that in vehicular ad hoc networks (VANET), it is possible to locate and track a vehicle based on its transmissions, during communication with other vehicles or the road-side infrastructure [5].This type of tracking leads to threats on the location privacy of the vehicle's user. In this paper, we study the problem of providing location privacy in VANET by allowing vehicles to prevent tracking of their broadcast interactions. We primary, classify the unique characteristics of VANET that must be considered when designing suitable location privacy solutions. In other related VANET security work, Golle et al. address the problem of an adversary injecting malicious data into the network, and propose a general approach to evaluating the validity of the data, where every node searches for possible descriptions for the data it has received and collected[6][7].

A potential approach for secure key distribution would be to empower the Department of Motor Vehicles (DMV) to catch the role of a Certificate Authority (CA) and to certify every

vehicle's public key. Unfortunately, this approach has multiple shortcomings [8] [9]. Initially, assuming the responsibility of a CA is a challenging process which is not in line with the DMV's present functionality. Extensive anecdotal evidence suggests that even specialised CAs offer questionable protection against dedicated attackers trying to acquire a certificate for another institution or entity. Second, vehicles from different states or different countries may not be able to authenticate every other unless vehicles trust all CAs, which reduces protection. Finally, certificate based key establishment has the danger of violating driver privacy, as the vehicle's identity is revealed during each key establishment. To create an anonymous identity, the vehicle generates a new public key pair {K, K−1} and sends a request for a new certificate for the public key K to a Certificate Authority. Vehicle would sign the request with its identity key KV and include the certificate C with the request [10]. Assuming the CA trusts the vehicle's manufacturer, it can authenticate the signatures and issue a limited-lifetime certificate for K that is unlikable (except by the CA) to the vehicle's actual identity. In addition, the CA should not issue overlapping unknown identities to the same vehicle (to prevent Sybil attack), so creating a decentralized system may be challenging [11] [12].

Efficient and easy-to-manage privacy and security enhancing mechanisms are necessary for the wide spread acceptance of the VANET technology. In this paper, we are concerned with this problem; and in particular, how to achieve efficient and robust pseudonym-based authentication [13]. We design mechanisms that reduce the security overhead for safety beaconing, and retain robustness for transportation protection, still in adverse network settings. Furthermore, we illustrate how to enhance the usability and availability of privacy-enhancing VANET mechanisms: Our proposal permits vehicle on-board units to produce their own pseudonyms, without affecting the system protection [14].

A Public Key Infrastructure (PKI) can provide this functionality using certificates and fixed public keys. Though, fixed keys permit an eavesdropper to connect a key with a location and a vehicle, violating drivers' privacy. In this work we propose a VANET key management scheme based on Temporary Anonymous Certified Keys (TACKs). Our method efficiently prevents eavesdroppers from linking a vehicle's different keys and gives timely revocation of misbehaving participants while maintaining the less or same overhead for vehicle-to-vehicle communication as the current IEEE 1609.2 standard for VANET security [15].

3. Current Approach:

This section represents the available approaches in privacy-preserving scheme to detect the Sybil attacks in Vehicular Ad hoc Networks. We propose a privacy-preserving scheme to detect the Sybil attacks in VANET's. The RSB is securely connected to the DMV via a backhaul wired network. Our scheme DMV provides vehicles with a pool of pseudonyms that are used for hiding the vehicle's unique identity. To prevent a vehicle from using multiple pseudonyms to direct a Sybil attack, the pseudonyms is assigned to a particular vehicle are hashed to a common value (One Way Hash Function).

Network Topology:

Each node sends "hello" messages to allow other nodes to detect it. Once a node detects "hello" messages from another node (neighbours), it maintains a contact record to store information about the neighbours. Using multicast socket all nodes are used to detect the

neighbour's nodes. In the mobility, tables of connectivity, link reliabilities and DMV and RSB pointers are updated at Vehicles via the soft state process.

DMV Determining Hash Function:

The DMV knows the total number of vehicles, and sequentially produces a sufficient amount of yearly pseudonyms for all the vehicles. After producing a pseudonym p, the DMV first hashes (p | κc) using a one-way hash function, where κc is a global key. It afterwards chooses a set of bits from the hashed outcome to generate hash collisions. The particular bits are referred as "coarse-grained hash value". Subsequently, the pseudonym p is placed into a group, which stores the pseudonym through the same coarse-grained hash values. In other words, for each pseudonym pl in the m^{th} coarse-grained group, we have H (pl|κc) = Γm, where H is a one-way hash function, and Γm is the coarse-grained hash value for group m. We refer such groups as "coarse-grained groups". The key κc will be distributed to all the RSBs. Similarly, the DMV calculates the hash value for the above p. With a new key κf and calculate the fine-grained hash value (Θn) for the group.

RSB Verification Process:

When vehicles communicate, an RSB overhears all the vehicles within their communication range and collects the all the pseudonyms for the event. The RSB goes through each pseudonym p and computes the coarse-grained hash value H (p|κc). Then the RSB notices that two pseudonyms of the same coarse grained hash value are used to sign the event. This can be either (i) a Sybil attack or (ii) a false alarm, The RSB cannot discriminate between (i) and (ii) and it sends the report to the DMV. The report contains the event, the pseudonyms whose coarse-grained hash value is Γ, the signatures of the event, and the certificates accompanying the pseudonyms.

DMV Verification Process:

On receiving an RSB report, the DMV first verifies the signatures and the coarse-grained hash value Γ to prevent a compromised RSB. If the RSB proves to be bonafide, the DMV calculates the fine grained hash value H (p|kf) for each pseudonym p in the RSB report. If the report such that same, the DMV concludes from the same vehicle that has attempted a Sybil attack. The DMV then takes further action to punish or revoke the malicious vehicle.

Performance Verification:

The DMV loads a unique fine-grained group of pseudonyms to each vehicle at the time of yearly vehicle registration, and stores the corresponding the vehicle's secure plate number. It is obvious that the mapping from secure plate numbers to vehicles is one-to-one. Thus, the DMV needs to carefully choose the length of the total number of available secure plate numbers are greater than or equal to the number of vehicles. The two-level hashing saves storage for the DMV, because the DMV can link a pseudonym to a vehicle by calculating its coarse-grained and fine-grained hash values, and then comparing them with the secure plate number. This obviates the need of maintaining vehicle secure plate numbers and pseudonym association. After the initialization stage, the DMV stores the secure plate number for each vehicle, and secretly keeps the fine grained hash key κf. When generating the pseudonyms, we need to consider the lifetime of a coarse-grained key κc, because an attacker gaining access to an RSB can partially learn the pseudonyms of all the vehicles for that lifetime. If

the lifetime is too long, the privacy of the vehicles will be severely impaired. RSB holds each valid coarse-grained key only for a short time. When an RSB is compromised, the attacker only obtains the coarse-grained hash key for the current time interval. We do not impose any restrictions on the fine-grained key κf , because the DMV does not release it, and an attacker cannot obtain it by compromising an RSB. Comparing to the long-period keys, this short-period key generation uses Ω coarse-grained hash keys instead of one, thus bringing an extra storage overhead to the DMV. The DMV then takes further action to punish or revoke the malicious vehicle. In this scheme, a Sybil attack is guaranteed to be detected. However, when the vehicles are densely distributed, false alarms can happen often.

The architecture Fig.1 involves DMV, RSB's and vehicles. Here DMV (Department of Motor vehicle) is the centralized one which is responsible for all the events that took place during the transaction.DMV creates the number of RSB's (Road Side boxes) within the range. On the other hand vehicles are also created within the range. Then all the RSB's and vehicles are connected to the DMV. DMV generates pseudonyms for all the vehicles. When a vehicle communicates with each other RSB's overhears all the vehicles pseudonyms within the range and calculates the coarse-grained value for the entire vehicle within their range. Since RSB's cannot discriminate whether the Sybil attack has happened are not so it just forwards the data to the DMV. The DMV receives the RSB's request and calculates the fine-grained value for the vehicles if the values are same then the DMV concludes that Sybil Attack has been happened and it removes the vehicle from the further transactions.

If the values of fine-grained are different for the vehicles DMV approves the further transactions and sends the report to the RSB's. The RSB's receives the DMV request and transfers the information directly to the vehicles. The vehicle receives the data successfully from the RSB's. Finally the data has been sent and received successfully.

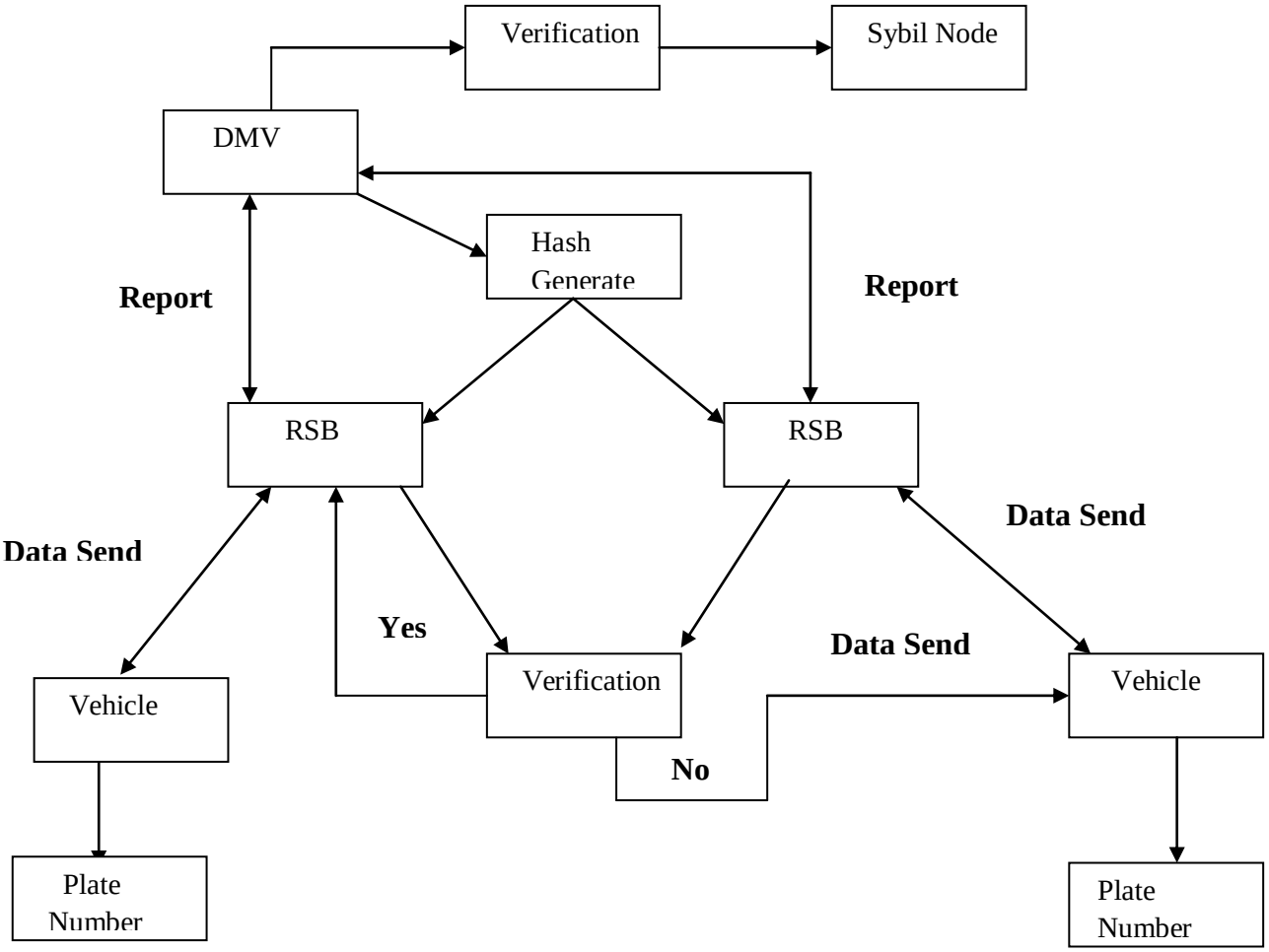

Fig.1. Architecture Diagram

4. Conclusion

The proposed method distributes the computation workload from the DMV to RSBs while releasing only a limited amount of information by using hash collusions. We also discussed some improvements on our scheme. Based on simulation results presented, we prove that the idea of distributing DMV workload to RSBs with limited information released is applicable in other VANET security and privacy applications. One interesting future work is to develop a machine learning algorithm to predict the ratio and activities of malicious vehicles. With a good estimation of the ratio of attackers, P2DAP is expected to efficiently catch attackers with a small overhead and delay. Besides, the DMV can be involved for a centralized management of resources during the detection. Furthermore, the DMV can be distributed to different areas such as regional DMV, which matches the case in real life, and forms a more powerful structure.

References

1. Enkelmann, W. “Fleetnet-applications for inter-vehicle communication”. In Intelligent Vehicles Symposium, 2003. Proceedings. IEEE, pp. 162-167, June 2003.
2. Kosch, T. I. M. O., and M. A. R. K. U. S. Strassberger. "The role of new wireless technologies in automotive telematics and active safety." 8th Symposium Mobile Communications in Transportation. 2004.
3. El Zarki, Magda, Sharad Mehrotra, Gene Tsudik, and Nalini Venkatasubramanian. "Security issues in a future vehicular network." In European Wireless, vol. 2. 2002.
4. Li, Mingyan, R. Poovendran, K. Sampigethaya, and L. Huang. "Caravan: Providing location privacy for vanet." In Proc. Embedded Security in Cars (ESCAR) Workshop, vol. 2, pp. 13-15, 2005.
5. Choi, Jong Youl, Markus Jakobsson, and Susanne Wetzel. "Balancing auditability and privacy in vehicular networks." In Proceedings of the 1st ACM international workshop on Quality of service & security in wireless and mobile networks, pp. 79-87. ACM, 2005.
6. Calandriello, Giorgio, Panos Papadimitratos, Jean-Pierre Hubaux, and Antonio Lioy. "Efficient and robust pseudonymous authentication in VANET." In Proceedings of the fourth ACM international workshop on Vehicular ad hoc networks, pp. 19-28. ACM, 2007.
7. Rass, Stefan, Simone Fuchs, Martin Schaffer, and Kyandoghere Kyamakya. "How to protect privacy in floating car data systems." In Proceedings of the fifth ACM international workshop on VehiculAr Inter-NETworking, pp. 17-22. ACM, 2008.
8. Parno, Bryan, and Adrian Perrig. "Challenges in securing vehicular networks." In Workshop on hot topics in networks (HotNets-IV), pp. 1-6. ACM, 2005.
9. Studer, Ahren, Elaine Shi, Fan Bai, and Adrian Perrig. "TACKing together efficient authentication, revocation, and privacy in VANETs." In 2009 6th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, pp. 1-9. IEEE, 2009.
10. Golle, Philippe, Dan Greene, and Jessica Staddon. "Detecting and correcting malicious data in VANETs." In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 29-37, 2004.
11. Raya, M., & Hubaux, J. P. Securing vehicular ad hoc networks. Journal of Computer Security, 15(1), 39-68, 2007.
12. Raya, M., Jungels, D., Papadimitratos, P., Aad, I., & Hubaux, J. P. “Certificate revocation in vehicular networks”. Laboratory for computer Communications and Applications (LCA) School of Computer and Communication Sciences, EPFL, Switzerland, 2006.
13. Suh, W., Yun, H., Chon, K. S., & Park, C. H. “Forecasting hourly traffic volume of airport access road: Case study of incheon international airport”. 2005 Annual Transportation Research Boards’ (TRB) Meeeting, 2005.
14. P. Flajolet, D. Gardy, and L. Thimonier, “Birthday paradox, coupon collectors, caching algorithms and self-organized search,” Discrete Applied Mathematics, vol. 39, pp. 207 – 229, 1992.
15. Sweeney, L. (2002) “k-anonymity: A model for protecting privacy”, International Journal on Uncertainty. Fuzziness and Knowledge-based Systems, vol.10, no.5, pp.557–570.