A Novel Security Scheme in VANET using ASIA

B.Arigengaram, J. Rethna virgil Jeny, J. Albert Simon

Abstract — A vehicular ad hoc network (VANET) uses cars as mobile nodes in a MANET to create a mobile network. In the vehicular ad hoc networks the security is an important concern. For security purpose, Vehicular ad hoc networks (VANETs) adopt the Public Key Infrastructure (PKI) and Certificate Revocation Lists (CRLs).This PKI system, the authentication of a received message is performed by checking if the certificate of the sender is included in the current Certificate Revocation Lists (CRLs) and verifying the authenticity of the certificate. But it takes more time for CRL checking process. So, in order to overcome this problem a keyed Hash Message Authentication Code(HMAC) is used. In addition, EMAP uses a novel probabilistic key distribution, which enables non-revoked OnBoardUnits to securely share and update a secret key. By using this method the message loss ratio is significantly reduced. But in this method generating and verifying such signatures can cause high computational overhead. So, to conquer this trouble an innovative technique called ASIA (Accelerated secure in-network aggregation)is introduced. ASIA can largely accelerate message verifications and drastically reduce computational and communication overhead compared to existing schemes.

Key words — VANET, Vehicle to Vehicle Communication, RSU,OBU, ECDCA,ACC,GSV

1 AVEHICULAR AD-HOC NETWORK (VANET)

VANET is a self-configuring infrastructure less network of mobile devices connected by wireless links. Each device in a VANET is free to move independently in any direction, and change its links to other devices frequently. Each device must forward traffic unrelated to its own usage, and therefore be a router. The primary challenge in building a Vehicular ad hoc network is equipping each device.

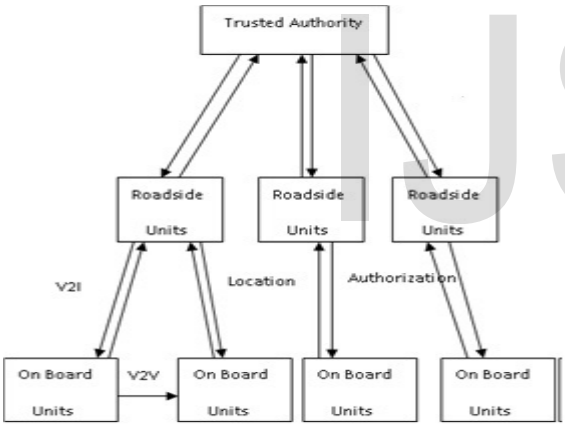

Fig. 1 VANET Architecture

It continuously maintained the information required to properly route traffic. Some networks may operate by themselves connected to the larger Internet. VANETs are a kind of wireless ad-hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network.

2 INTRODUCTION

The main goal of this work is to improve the security concerns in data aggregation in VANETs. VANETs have several unique characteristics that contribute to the difficulties in designing secure aggregation strategies, including highly dynamic network topology, transitory nature of interactions, absence of centralized authority and low tolerance for errors. Existing approaches regard digital signatures as the building block of secure data aggregation[6][7]. In IEEE 1609.2 standard[10] , Elliptic Curve Digital Signature Algorithm (ECDSA) is used to provide authentication and non-repudiation. Generating and verifying signatures using ECDSA, however, leads to high computational overhead on the On-Board Unit (OBU) that validates messages. A typical OBU with a 400 MHz processor needs 20 milliseconds to verify one ECDSA signature. Given that beacon messages are broadcast every 100 milliseconds, a vehicle with more than 5 neighbors around cannot timely verify incoming messages. Therefore, even in a benign scenario, vehicles are likely to be overwhelmed, let alone the scenario with malicious neighbors. This potentially allows signature flooding attacks. Also, signatures can causes excessive transmission overhead, especially in aggregation scenario where nodes may concatenate downstream signatures to create considerably long messages. Secure aggregation was first studied in the context of stationary sensor networks. Due to the static topology, sensors can set up secret symmetric keys among them to facilitate security mechanisms. In this approach broadcast authentication is guaranteed using TESLA, so that nodes can authenticate messages. To secure aggregation, each node generates a commitment to its aggregates which is verifiable to the querier. This scheme has multiple runs of information dissemination which require a relatively stable network topology. In this work preloaded symmetric keys at each sensor. In these schemes symmetric cryptography is preferred against signatures to reduce overhead.

To secure aggregation in VANETs, symmetric cryptography is also applied. Recent research has proposed several alternatives to the heavyweight signature strategy. In this scheme nodes evaluate the trustworthiness of the aggregates using selective attestation and trust management. The proposed probabilistic scheme uses the FM-sketch data function and symmetric cryptography to generate lightweight authentication codes. However, these schemes rely on pre-distribution of symmetric keys, which is considered non-realistic for VANET applications. It incurs key management issues. ASIA is designed as an effective and efficient scheme for securing data aggregation in Vehicular ad hoc network. This approach can dramatically accelerate message verification faster than the

digital signature scheme. It is able to largely reduce the communication and computational overhead compared to various different strategies. ASIA consists of below two basic security mechanisms:

1.Aggregate Consistency Check (ACC)

2 Generation-Skipping Verification(GSV).

The main idea in designing ACC is providing security through introducing redundancy into the aggregation data flow. In this design directed acyclic graph (DAG)[6] as the aggregation structure instead of the commonly used tree graph. In this design, when performing aggregation in a DAG, one node sends its messages to various to upstream nodes. Messages with identical content flow via network and will reach eventually a common node which can compare the received messages to detect potential misbehavior during the aggregation process. However, constructing the desired DAG in VANETs is non-trivial. In this proposed approach, vehicles will leverage location and speed information already used for safety applications to facilitate DAG construction.
GSV builds upon TESLA is a lightweight broadcast authentication scheme. It allows upstream nodes in the aggregation structure to directly verify the integrity of messages from downstream nodes that are two hops away, bypassing the nodes residing between them. The philosophy of this approach is time-asymmetry authentication. The timing of message generation, packet transmission and secret key disclosure can offer authentication of source and message. In the method, expensive asymmetric cryptography can be avoided for most of the time.

3 ASIA VERIFICATION COMPONENTS

3.1 Aggregate Consistency Check

In previous work on aggregation security in VANETs, in-network aggregation is performed based on the tree structure. One benefit of this structure is its duplicate-free nature that can prevent double counting. In addition, there are many mature spanning tree construction algorithms. In this paper, the directed acyclic graph (DAG) is proposed to replace the spanning tree as the aggregation structure. Aggregation in DAG differs in the sense that each node except the root, rather than sending its message to only one upstream node, will transmit it to two or more nodes. Receivers separately compute an aggregate and then send it with their own reading to a same upstream node which can thus check the integrity by comparing received messages. This proposed aggregate consistency check (ACC), which verifies the aggregates of other nodes using the atomic consistency block (ACB). An ACB is defined by four nodes: A, pi(A) and pj(A) (i, j = 1, · · ·, nAp and i 6= j) such that P(pi(A)) \ P(pj(A)) is non-empty, and a verifier vij(A) 2 P(pi(A))\P(pj(A)). Then the block is defined as ACB(A) ={A, pi(A), pj(A), vij(A)}.In a consistency check, vij(A) compares two aggregates coming from pi(A) and pj(A).For example, node A sends its reading 7 to pi(A) and pj(A) whose own readings are 3 and 8, respectively. Each node then computes the SUM aggregate which is sent to node D with its own reading. So vij(A) will receive (10, 3) from pi(A), and (15, 8) from pj(A). By subtracting the reading from the aggregate, vij(A) can obtain the actual data from A separately from these two messages. If pi(A) and/or pj(A) misbehave fabricating the aggregate, vij(A) can detect any inconsistency after the subtraction operation. One thing the attacker can do is falsify the aggregate and modify its own reading as well to ensure the subtraction remain the same. This attack is equivalent to modifying its own sensory readings. The DAG offers the possibility of locally detecting misbehavior, at the price of complexity in constructing the aggregation structure.

3.2 Generation Skipping Verification

If pi(A) and pj(A) do not collude when they are trying to falsify their aggregates, there is strong probability that their data will result in inconsistency at node vij(A). If pi(A) and pj(A) do collude and add a same value to their aggregates. Then the messages received by vij(A) may look like (90, 3), (95, 8), which can bypass the current 'aggregate consistency check' security scheme. Given the legitimate aggregates (10,3) and (15,8), collusive attack 1 can totally subvert the final result. To detect aggregate manipulation attack even with collusion existing, it is favorable that node vij(A) is able to directly verify the reading at A. A straightforward approach is to establish a shared secret between A and vij(A). This can be done with Diffie-Hellman key exchange protocol or any appropriate method. This method, however, incurs high communication and computational overhead and may be infeasible in the VANETs scenario. Threats during DAG construction. The proposed Generation Skipping Verification (GSV) which makes it possible that the verifier at the upper end in ACB can verify the integrity of readings from the source node at the lower end, even in the presence of possibly malicious nodes at the middle tier. Symmetric cryptography is used in our scheme for most time to accelerate message verification and reduce overhead.

4 ASIA ALGORITHMIC FRAMEWORK

4.1 Group Formation and Management

Vehicles in the network are arranged into groups. After the aggregation is triggered, vehicles first determine the group the belonging to grouping is location-based. The road is dissected into small sections. Which basically define different groups. A vehicle equipped with GPS can automatically know its group by comparing its GPS position to the preloaded road map with sections indicated.

4.2 Location-aware Aggregation Tree Construction

To construct the aggregation structure vehicles in each group first construct a spanning tree. They will face several challenges when trying to construct a preferable tree that can facilitate subsequent procedure. Classic distributed spanning tree algorithms might generate a random tree structure whose topology is unexpected. Recall that in our scheme, the aggregator A should connect to one of its parent's siblings C to generate the ACB. If the spanning tree is generated without any constraints, the random topology may result in communication failure between A and C. They might be physically far apart from each other and out of transmission range. A vehicle in the network can increase its transmission power in case that its desired parent is out of range. Maximum transmission radius is as high as 250 m. However larger transmission radius incurs more communication overhead and more severe contention over the wireless medium. Therefore, it is not desirable to increase transmission power to reach a far away parent. The tree construction algorithm should ensure that logically close nodes in the aggregation DAG are also geographically close to each other. Given the feature vehicles can construct the aggregation tree along the moving direction of traffic. The tree will not span in arbitrary directions so that physical locations of vehicles will basically match their logical positions in the aggregation structure.

4.3 Relative Position Detection

Each vehicle needs to determine the relative position between itself and neighbors. They can leverage the location information embedded in the periodically broadcast beacon.

4.4 Lane Identification

Knowing the lane on which neighbors are running, vehicles can construct a more stable tree structure that maintains better connectivity. In some time, the Car pool lane has much faster traffic while the outermost lane has slow traffic. Lane number information will be considered when choosing parent node.

5 CONCLUSION

This paper maintains the secure and efficient data aggregation in VANET as a sensing platform. ASIA can largely accelerate message verifications and dramatically reduce computational and communication overhead compared to existing schemes like EMAP. ASIA can significantly decrease the message loss ratio due to message verification delay compared to the conventional authentication methods employing CRL checking.

REFERENCES

[1] T. Willke, P. Tientrakool, N. Maxemchuk, "A Survey of Inter-Vehicle Communication Protocols and Their Applications," Communications Surveys and Tutorials, IEEE , vol.11, no.2, pp.3-20, Second Quarter 2009.

[2] U. Lee, M. Gerla, "A Survey of Urban Vehicular Sensing Platforms," Computer Networks, Volume 54, Issue 4, Pages 527-544, ISSN 1389- 1286, March 2010.

[3] S. Dietzel, F. Kargl, G. Heijenk, and F. Schaub, "Modeling in-network aggregation in VANETs," Communications Magazine, IEEE , vol.49, no.11, pp.142-148, November 2011.

[4] C. Lochert, C. Wewetzer, A. Luebke, and M. Mauve, "Data Aggregation and Roadside Unit Placement for a VANET Traffic Information System," in Proceedings of the fifth ACM international workshop on Vehicular Inter-NETworking (VANET '08). ACM, New York, NY, USA, 2008.

[5] B. Parno, and A. Perrig, "Challenges in Securing Vehicular Networks," in Proc. of the Workshop on Hot Topics in Networks (HOTNETS-IV), 2005.

[6] J. Molina-Gil, P. Caballero-Gil, C. Herna, and C. Caballero-Gil, "Data Aggregation for Information Authentication in VANETs," in 6th International Conference on Information Assurance and Security, Aug. 2010.

[7] M. Raya, and J. Hubaux, "Securing Vehicular Ad Hoc Networks," Journal on Computer Security, 15(1): 39-68, Jan. 2007.

[8] N. Ristanovic, P. Papadimitratos, G. Theodorakopoulos, J.-P. Hubaux, and J.-Y. Leboudec, "Adaptive Message Authentication for Vehicular Networks," in Proc. of ACM VANET '09, 2009.

[9] M. Raya, A. Aziz, and J. Hubaux, "Efficient Secure Aggregation in VANETs," in ACM VANET '06, New York, NY, USA, 2006.

[10] IEEE, "1609.2-2006: IEEE Trial-Use Standard for Wireless Access in Vehicular Environments-Security Services for Applications and Management Messages," IEEE Standard, 2006.

[11] H.-C Hsiao, A. Studer, C. Chen, A. Perrig, F. Bai, B. Bellur, and A. Iyer, "Flooding-Resilient Broadcast Authentication for VANETs," in Proc. ACM MobiCom 11, 2011.

[12] S. Dietzel, E. Schoch, B. Konings, M. Weber and F. Kargl, "Resilient Secure Aggregation for Vehicular Networks," IEEE Journal on Network Management of Global Internetworking, Jan. 2010.

[13] Q. Han, S. Du, D. Ren, and H. Zhu, "SAS: A Secure Data Aggregation Scheme in Vehicular Sensing Networks," in Proc. IEEE ICC, 2010.

[14] H. Chan, A. Perrig, and D. Song, "Secure Hierarchical In-Network Aggregation in Sensor Networks," in Proc. of the 13th ACM Conference on Computer and Communications Security, CCS '06, 2006.

BIOGRAPHIES

B.Arigengaram received his B.E degree in Computer Science and Engineering from Anna University, Chennai in 2011 and He is currently

doing M.E in Computer science and Engineering at Anna University.His research interest includes Vehicular Ad-hoc NETWORK in Networking.

J.Rethna Virgil Jeny received her B.E and M.E degrees in Computer Science and Engineering from Bharathidasan University, 1997 anan Trichy in and Annamalai University in 2005 espectively. She is currently doing Ph.D in wireless sensor Networks at MS University. She has received Lady Engineer Award by IEI. She is a member of IEEE, ACM, ISTE, IEI, IAENG and a senior member of IACSIT. Her research interests include Energy aware routing and Cross layer routing in Wireless Sensor Networks.

J. Albert Simon received his B.E. in Computer Science and Engineering from Anna university, Tirunelveli with Distinction in 2011 and ME in Computer Science and Engineering from Annauniversity, Chennai with distinction in 2013.He has secured fifth rank in Anna University M.E Examination. He has presented papers in International and National Conferences. His research interest includes Wireless Mesh Networks and Network Security.