A DTSA (Detection Technique against a Sybil Attack) Protocol using SKC (Session Key based Certificate) on VANET

ByungKwan Lee[1], EunHee Jeong[2] and Ina Jung[3]

[1]Department of Computer, College of Engineering, Kwandong University, Gangneung-si, Gangwon-do 210-701, Korea
[2]Department of Regional Economics, College of Humanity & Social Science, Kangwon National University, Samcheok, Gangwon-do, 245-711, Korea
[3]Department of Computer Science, College of Engineering, Kwandong University, Gangneung-si, Gangwon-do 210-701, Korea

[1]bklee@kd.ac.kr, [2]jeongeh@kangwon.ac.kr, [3]lupinus07@nate.com

Abstract

This paper proposes a DTSA(Detection Technique against a Sybil Attack) protocol so that it can provide vehicles with the secure information for the road situation and the traffic flow among vehicles and by detecting a Sybil attack. This DTSA uses SKC(Session Key based Certificate) to verify the IDs among vehicles, which generates a vehicle's anonymous ID, a session key, the expiration date and a local server's certificate for the detection of a Sybil attack. In conclusion, this DTSA reduces not only the detection time against a Sybil attack but also the verification time for ID by using a hash function and an XOR operation. Besides, a drivers' privacy can be protected by using an anonymous ID. This DTSA helps drivers drive safely with the reliable information of VANET and reduce traffic accidents.

Keywords: *DTSA, SKC, Sybil attack, VANET, Anonymous ID*

1. Introduction

Recent advances in wireless networks have led to the introduction of a new type of networks called VANET (Vehicular Ad hoc Networks). There are many envisioned applications for VANET: vehicle safety enhancement, traffic congestion notification and emergency notification [1, 2, 3].

Sybil attack was first introduced by Douceur in the context of peer-to-peer networks [4]. It allows a malicious sender to create multiple fake identities (called Sybil nodes) to impersonate as normal nodes. Most VANET based applications, such as cooperative forward collision warning, pre-crash sensing and warning, local hazard notification, need the cooperation of vehicles. Sybil attack is particularly harmful due to violate the fundamental assumptions of the VANET research [5, 6].

This paper uses SKC (Session Key based Certificate) as the method for validating IDs communicating between vehicles to detect a Sybil attack. Therefore, this paper provides more safe transportation by safely exchanging the messages for the road situation and the traffic flow between vehicles for VANET by detecting a Sybil attack.

[1] First Author
[2] Corresponding Author

2. Related Works

2.1. VANET

There are two types of nodes in VANET; mobile nodes as OBUs (On Board Units) and static nodes as RSUs (Road Side Units). An OBU resembles the mobile network module and a central processing unit for on-board sensors and warning devices. The RSUs can be mounted in centralized locations such as intersections, parking lots or gas stations. They can play a significant role in many applications such as a gate to the Internet [6].

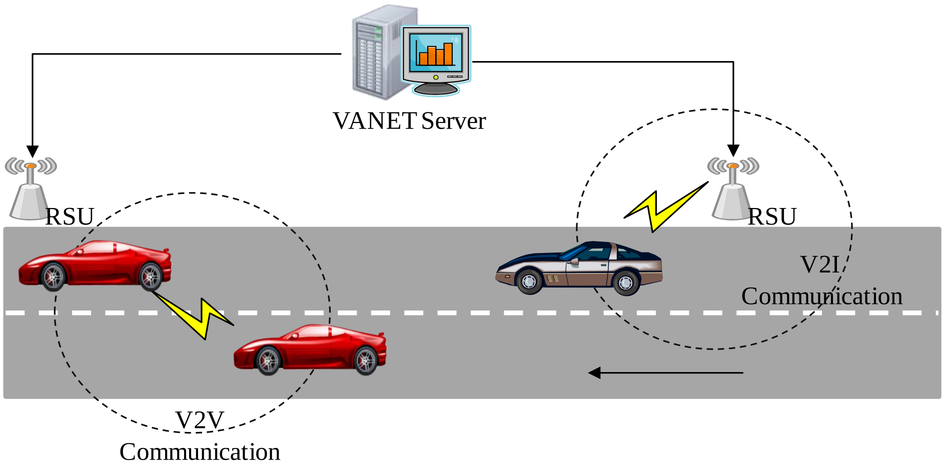


Figure 1. The inter-vehicle communication and the components involved

Figure 1 illustrates a typical VANET. A vehicle is enabled with an on-board communication unit for V2V (Vehicle to Vehicle) and V2I (Vehicle to Infrastructure) communications, and sensors (for example, GPS) and database units to collect environmental information (for example, vehicle location, vehicle speed, tire pressure). The communication unit of the access points are called RSU, which are connected to a VANET server by a wired network. The VANET server records all the data forwarded by the RSUs, and processes the data together with information from other data sources, for example, vehicle manufacturers, police, traffic management centers, and weather information centers [7, 8].

Vehicles move on roads, sharing collective environmental information between themselves with the servers via access points. As VANET’s V2I is the communication between vehicles and a trust authority, the security technique of the existing network must be used in it. But, VANET’s V2V is the communication between vehicles without a trust authority, some security problems can happen in it. If only one accidents happen, it leads to casualties. It is important for VANET to guarantee safe and reliable communication due to the nature of VANET. Therefore, VANET’s communication protocols have to satisfy the securities requirements such as the authentication, the integrity, the non-repudiation, and the conditional anonymity of messages [9].

As this paper generates the local certificate based on a session key for validating vehicles without violating vehicles’ privacy by using conditional anonymity, it provides reliable services with VANET. Therefore, drivers drive safely with VANET’s information and reduce traffic accidents.

2.2. Sybil attack

VANET supports the services associated with drivers' safety such as the information transmission between vehicles, the rear-end collision between vehicles, and the warning about dangerous situations in real time. In the Figure 2 [10, 11], the attacker who disguised itself as ID A sends wrongly the messages such as the information transmission between vehicles, the rear-end collision between vehicles, and the warning about dangerous situations. It throws other vehicles into confusion. That is, as the objective of a Sybil attack is to make other vehicles change the route on the road or leave the road for the attacker, a Sybil attack can be a serious threat because it causes great damage to a VANET's function.

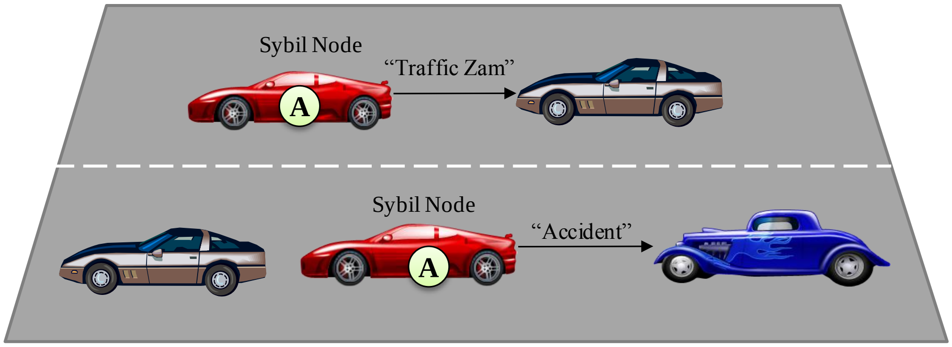


Figure 2. Sybil Attack

The DTSA in this paper is designed to use the local certificate based on a session key as the method for validating the IDs between vehicles to detect a Sybil attack. It also provides driver's safety by safely transmitting the reliable messages such as the information transmission between vehicles, the rear-end collision between vehicles, and the warning about dangerous situations.

3. DTSA Design

As this proposed DTSA assumes that all vehicles have a hash function, ECC algorithm, AES algorithm, a master key, and an unique ID. It is designed so that a Sybil attack can be detected by validating drivers' ID which exchanges messages among vehicles by using SKC. The total flowchart of DTSA is shown in Figure 3, and the DTSA's step-by-step process is as follows [12].

First, vehicles' unique ID and master key are registered in a VANET server.

Second, vehicle A generates anonymous ID and sends it to a local VANET server which vehicle A belongs to.

Third, a local VANET server validates the anonymous ID of vehicle A in a VANET server.

Forth, vehicle A and a local VANET server generates a session key each. And they generates Vehicle A's local certificate with the session key.

Fifth, vehicle A sends the local certificate based on a session key, Road number, message and the message's hash value to vehicle B.

Sixth, vehicle B validates vehicle A's ID by requesting vehicle A's local certificate based on a session key to a local VANET server. If the authentication of vehicle A's local certificate based on session key is not correct, it is taken into account that a certain vehicle attacked vehicle B after stealing vehicle A's ID and it is called a Sybil attack. If vehicle B detects the Sybil attack, it sends the result to the local VANET server.

Seventh, if vehicle A's ID is validated, vehicle B which received vehicle A's message makes the hash value with the message. The message's integrity is validated by comparing vehicle B's hash value to the hash value which vehicle A sent.

Eighth, vehicle B validates the road number which vehicle A sent. And vehicle B checks whether vehicle A is on the same location as vehicle B. If the roads are overlapped on a boundary line, the road number must be selected in the light of vehicles' direction.

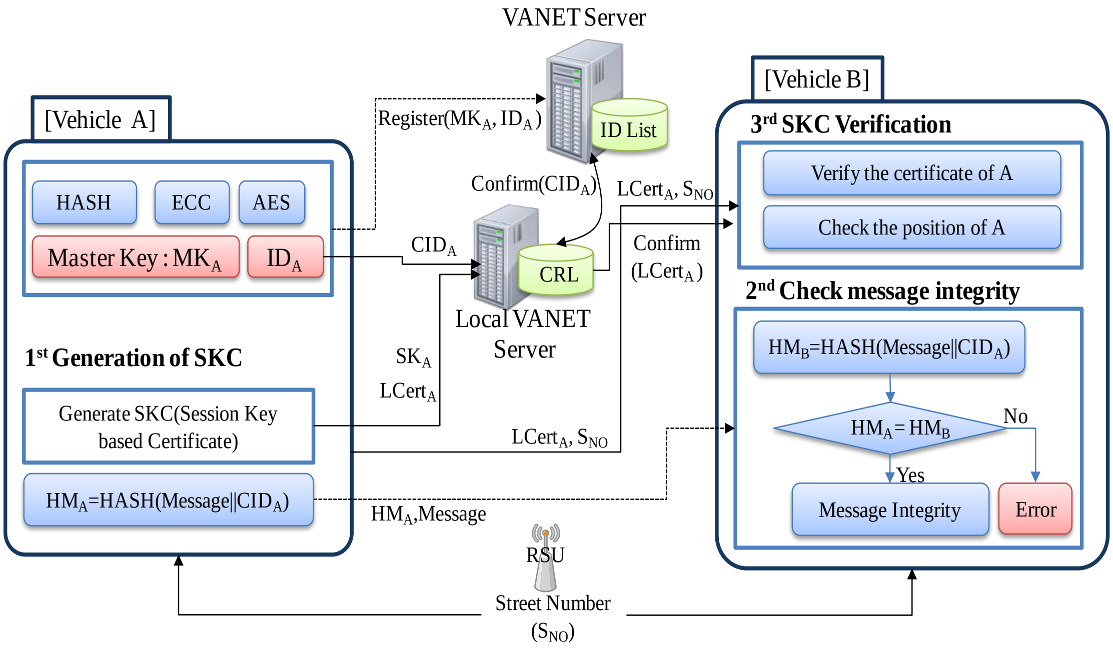


Figure 3. The total flowchart of DTSA

3.1. Generation of SKC

The DTSA generates SKC by using each vehicle's unique ID, a master key, a certificate's expiration date T, a private key, a public key and a local VANET's certificate. The generation flowchart is shown in Figure 4, the generation procedure is as follows.

First, vehicle A concatenates a master key, MK_A with ID_A, hashes the concatenated result, and generates CID(Commitment ID) which made vehicle A's ID anonymous. And vehicle A sends the CID_A to a local VANET server.

$$CID_A = \mathrm{HASH}(MK_A \mid\mid ID_A)$$

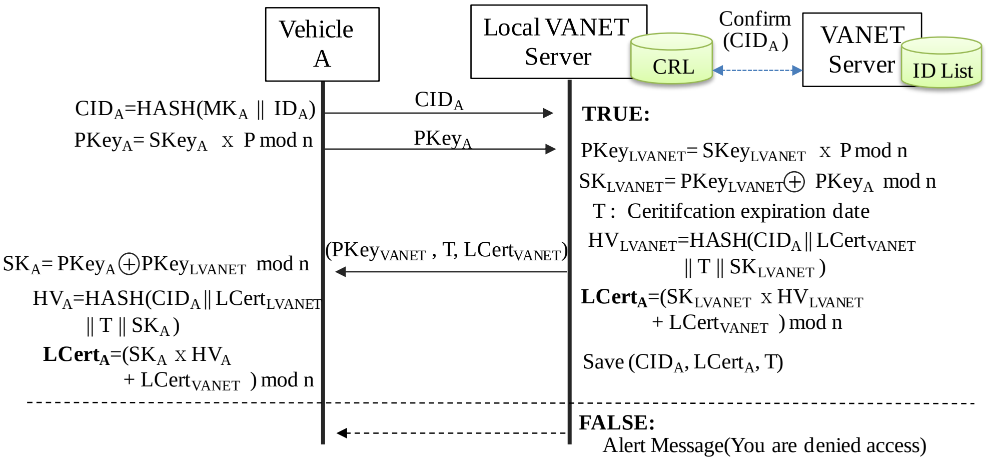

Vehicle A
Local VANET Server
CRL
Confirm (CID_A)
VANET Server
ID List
CID_A=HASH(MK_A || ID_A)
$PKey_A$= $SKey_A$ x P mod n
CID_A
$PKey_A$
TRUE:
$PKey_{LVANET}$= $SKey_{LVANET}$ x P mod n
SK_{LVANET}= $PKey_{LVANET}$ ⊕ $PKey_A$ mod n
T : Ceritifcation expiration date
HV_{LVANET}=HASH(CID_A || $LCert_{VANET}$ || T || SK_{LVANET})
($PKey_{VANET}$, T, $LCert_{VANET}$)
SK_A= $PKey_A$ ⊕ $PKey_{LVANET}$ mod n
HV_A=HASH(CID_A || $LCert_{LVANET}$ || T || SK_A)
$LCert_A$=(SK_A x HV_A + $LCert_{VANET}$) mod n
$LCert_A$=(SK_{LVANET} x HV_{LVANET} + $LCert_{VANET}$) mod n
Save (CID_A, $LCert_A$, T)
FALSE:
Alert Message(You are denied access)

Figure 4. The generation flowchart of SKC

Second, local VANET requests the validation for vehicle A's CID_A to a VANET server. If vehicle A's CID is in VANET, go to the next step. Otherwise, "access denial" message is transmitted to vehicle A, and the generation job of SKC is closed by force.

Third, vehicle A generates a public key($PKey_A$) about vehicle A's private key($SKey_A$) with an ECC algorithm and sends it to a local VANET server.

$$PKey_A=SKey_A \times P \ mod \ n$$

Fourth, a local VANET server generates a public key($PKey_{LVANET}$) about a private key($SKey_{LVANET}$).

$$PKey_{LVANET} = SKey_{LVANET} \times P \ mod \ n$$

Fifth, a local VANET server XORs a vehicle A's public key ($PKey_A$) and a local VANET server's public key($PKey_{LVANET}$) and generates a session key. And it hashes a certificate's expiration date T, a local VANET server's certificate ($LCert_{VANET}$), vehicle A's CID(CID_A), and a session key(SK) by hash function. A local VANET server multiplies the hash value by the session key, and generates vehicle A's SKC by adding the multiplied result value to a local VANET server's certificate. And (CID_A, $LCert_A$, T) is stored in CRL DB of a local VANET server.

$$SK_{LVANET} = PKey_{LVANET} \ XOR \ PKey_A \ mod \ n$$

$$HV_{LVANET} = \mathrm{HASH}(CID_A \ || \ LCert_{VANET} \ || \ T \ || \ SK_{LVANET} \ )$$

$$LCert_A = HV_{LVANET} \times SK_{LVANET} + LCert_{VANET} \ mod \ n$$

Sixth, a local VANET server transmits ($PKey_{LVANET}$, T, $LCert_{VANET}$) to vehicle A.

Seventh, vehicle A generates a session key with a local VANET server's public key which a local VANET server received.

$$SK_A = PKey_A \ XOR \ PKey_{LVANET} \ mod \ n$$

Eighth, vehicle A hashes the session key value of the sixth step and the T and $LCert_{VANET}$ which are received from a local VANET server by hash function.

$$HV_A = \mathrm{HASH}(CID_A \ || \ LCert_{VANET} \ || \ T \ || \ SK_A)$$

Ninth, vehicle A generates SKC. Vehicle A's SKC has the same value as the certificate in the fifth step.

$$LCert_A = HV_A \times SK_A + LCert_{VANET}\ mod\ n$$

3.2. Design of message integrity

As local VANET supports the services associated with drivers' safety, Vehicle B validates in DTSA whether the message which was received from vehicle A is safe or not. This paper is designed so that the message and it's hash value may be sent at the same time by using hash function stored in vehicle. The verification procedure of message integrity is as follows.

First, Vehicle A concatenates the message which will be transmitted to vehicle B and vehicle A's commitment ID(CID_A). Vehicle A hashes the concatenated result by hash function.

$$HM_A = \text{HASH}(Message \mid\mid CID_A)$$

Second, vehicle A transmits the commitment ID, the hash value of the first step, and message (CID_A, HMA, message) to vehicle B.

Third, vehicle B concatenates the message transmitted from vehicle A and vehicle A' commitment ID. Vehicle A hashes the concatenated result by hash function.

$$HM_B = \text{HASH}(message \mid\mid CID_A)$$

Fourth, vehicle B compares the HM_A transmitted from the second step with the hash value of the third step, HM_B and checks whether they match. If $HM_A \neq HM_A$, Vehicle B ignores it by judging that the message was forged.

3.3. Verification procedure of SKC

Figure 5 shows the verification procedure of the local certificate based on a session key. The verification procedure of SKC is as follows.

First, vehicle A sends vehicle A's commitment ID and SKC before transmitting a message to vehicle B.

Second, vehicle B generates the random number, nonce. Vehicle B sends the nonce and the CID_A transmitted from vehicle A to a local VANET server.

Third, a local VANET server leaves CID_A to a VANET server. If the CID_A is not in VANET server, a warning message meaning an unregistered vehicle is broadcasted to all vehicles within the VANET system.

Fourth, if vehicle A's CID_A is validated, a local VANET server detects SKC of CID_A in the CRL table and confirms the expiration date. And the hash value (HN_{LVANET}) which hashed the nonce received from vehicle B and the Vehicle A's SKC, $LCert_A^{LVANET}$ are transmitted to vehicle B.

Fifth, vehicle B checks whether the HN_B which hashed the nonce matches the HN_{LVANET} which is received from vehicle A match or not. If they don't match, vehicle B decides it is not a local VANET server and prints an error message.

Sixth, if the result of the fifth step is "TRUE", SKC sent from vehicle A is compared to the local server sent from a local VANET server. If the two certificates don't match, vehicle A is detected as a Sybil attack.

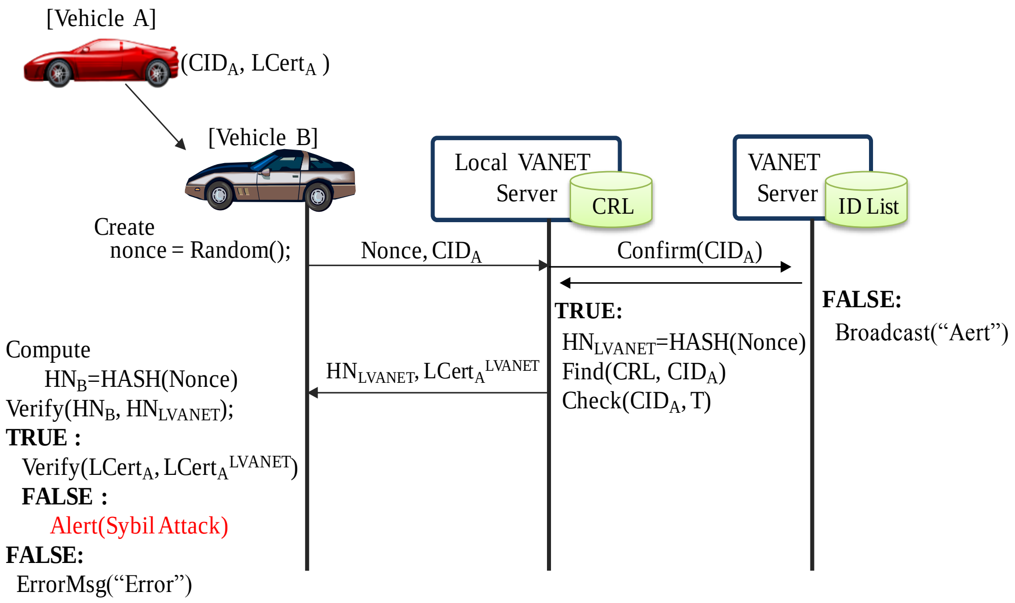


Figure 5. The verification process of SKC

4. Analysis

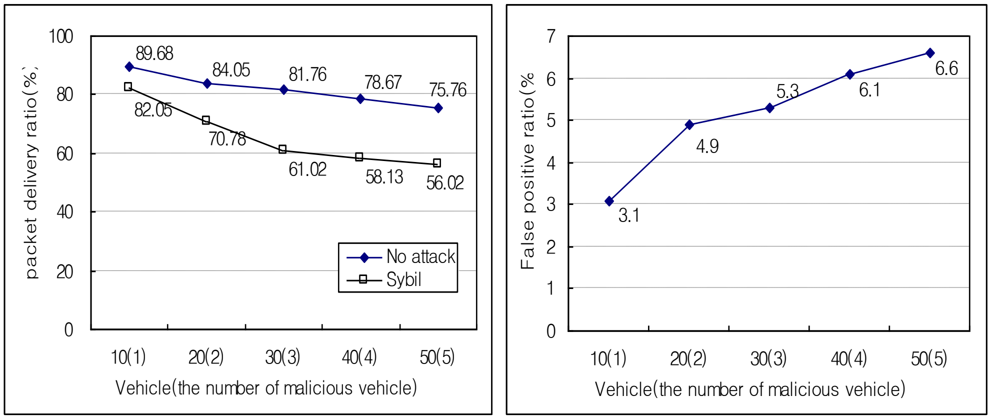
4.1. PDR and FPR Estimation

The simulation used an Intel(R) Core™ Duo CPU 2.99GHz 1.96GB RAM, and implemented on a Windows XP Home Edition operating system. To evaluate the effectiveness of the proposed DTSA in this paper, the DTSA is simulated using NS-2 simulator [13, 14]. The simulation parameter is shown in Table 1.

Table 1. Simulation parameter value for the DTSA

Parameter	Value
Simulation time	250sec
Number of normal node	45
Number of Sybil node	5
Transmission range	250m
packet size	512B
Packet sent by vehicles	1 per 5 second

This paper uses 45 normal nodes and 5 Sybil nodes and simulates a PDR(Packet Delivery Ratio) and a FPR(False Positive Ratio) for 250 seconds. The PDR means that the number of the packets received by a destination node is divided by the number of the packets sent by a source node.



(a) PDR(Packet Delivery Ratio) (b) FPR(False Positive Ratio)

Figure 6. The result of PDR and FPR estimation

As the DTSA doesn't transfer the nodes' packets with multi IDs to neighbor's nodes and deletes them, Figure 6(a) shows that it reduces the PDR regardless of the number of Sybil nodes increasing. The FPR means the ratio that the DTSA detects a normal node as a Sybil node. Figure 6(b) shows the experiment that the 10% of Sybil nodes was included in normal nodes. The result shows that the FPR is somewhat increased according to the increase of Sybil nodes.

4.2. Computation of data traffic

The DTSA exchanges the commitment ID, SKC, messages, the hash value between vehicles and between local VANET servers and validates vehicles' certificates. If the communication data generated by ECDSA algorithm are compared to the communication data generated by SAP for the validation of vehicles' certificates, ECDSA is 1,728bits and the DTSA is 1,152bits. And, the result of hash function is 160bit, that of ECC is 160bit, that of ECDSA's signature (r, s) is 320bit, and that of random nonce is 64bit [15, 16]. That is, the communication data of the DTSA is smaller than that of ECDSA.

$$\begin{aligned}\text{ECDSA} &= 4 \times 160(\text{public key}) + 2 \times 320(\text{signature}) + 5 \times 64(\text{nonce}) \\ &\quad + 2 \times 64(\text{Encode}) = 1{,}728\text{bits}\end{aligned}$$

$$\begin{aligned}\text{DTSA} &= 3 \times 160(\text{CID}_{\text{A}}) + 160(\text{LCert}_{\text{A}}) + 64(\text{nonce}) + 2 \times 64(\text{message}) \\ &\quad + 160(\text{hash}) + 160(\text{LCertA}_{\text{LVANET}}) = 1{,}152\text{bits}\end{aligned}$$

Also, ECDSA is 4M [17] and the DTSA is 2M. The DTSA is shorter than ECDSA in signature generation time, where M means multiply operation and the only multiply operation except other operations is used for signature generation time. Therefore, the DTSA is more efficient than existing ECDSA in data traffic, signature size, and signature generation time. In addition, the DTSA protects a vehicles' privacy by using anonymous ID, detects Sybil attack, and manages VANET efficiently.

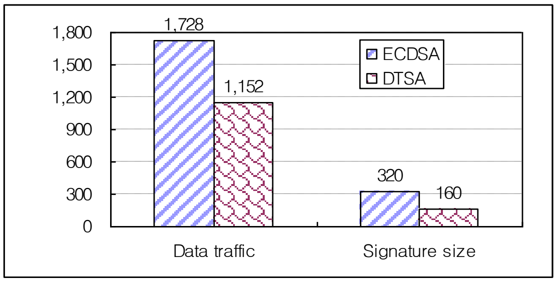


Figure 7. Comparison between DTSA and ECDSA

5. Conclusion

The services of VANET environment supports a drivers' safety such as the transmission of inter-vehicle information, the prevention of rear-end collision, and the warning about emergency and road condition through real time traffic information. This paper designs the DTSA that offers the conditional anonymity and the efficiency of VANET as follows.

First, the proposed DTSA generates SKC to validate inter-vehicle IDs.

Second, as the inter-vehicle IDs of the DTSA is validated with SKC, the Sybil attack stealing IDs can easily be detected.

Third, the DTSA protects a vehicles' privacy by using commitment ID.

Fourth, when a vehicle' certificate is validated in the DTSA, the processing time for the validation of vehicle's ID can be reduced with a simple hash function and XOR operation for the validation of vehicle's ID.

Fifth, as SKC of the DTSA is 160 bits long, the overhead of data communications can be reduced.

Sixth, as the integrity of message is verified, drivers drive safely with the reliable information.

Therefore, the reducing effect of traffic accidents can be expected.

References

[1] I. -H. Bae, "Design and Evaluaiton of a Hybrid Intelligent Broadcast Algorithm for Alert Message Dissemination in VANETs", Int'l Journal of Grid and Distributed Computing, vol. 4, no. 4, **(2011)**, pp. 1-10.

[2] A. Irshad, W. Noshairwan, M. Shafiq, S. Khurram, E. Irshad and M. Usman, "Security Enhancement for Authentication of nodes in MANET by checking the CRL status of Servers", International Journal of Advanced Science and Technology, vol. 22, **(2010)**, pp. 49-58.

[3] J. J. Hass, Y. -C. Hu and K. P. Laberteaux, "Real-World VANET Security Protocol Performance", GLOBECOM: IEEE, **(2009)**, pp. 1-7.

[4] J. R. Douceur, "The Sybil Attack", The First International Workshop on Peer-to-Peer System, LNCS, **(2002)**, pp. 251-260.

[5] S. Park, B. Aslam, C. Zou and D. Turgut, "Defense against Sybil Attack in Vehicular Ad hoc Network based on Roadside Units Support", Proceedings of Military Communications Conference(MILCOM'09), Boston, MA, USA, **(2009)** October 18-21.

[6] B. K. Chaurasia and S. Verma, "Infrastructure based Authentication in VANETs", International Journal of Multimedia and Ubiquitous Engineering, vol. 6, no. 2, **(2011)**, pp. 41-54.

[7] J. P. Hubaux, S. Capkun and J. Luo, "The security and privacy of smart vehicles", IEEE Security & Privacy, vol. 2, no. 3, **(2004)**, pp. 49–55.

[8] M. Raya and J. -P. Hubaux, "Security aspects of inter-vehicle communications", Proceeding of Swiss Transport Research Conference, Monte Verita / Ascona, **(2005)** March 9-11.

[9] K. Sampigethaya, M. Li, L. Huang and R. Poovendran, "AMOEBA: Robust Location Privacy Scheme for VANET", IEEE J. Select. Areas Communication, vol. 25, no. 8, **(2007)**, pp. 1569-1589.

[10] K. Konate and A. Gaye, "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc", International Journal of Future Generation Communication and Networking, vol. 4, no. 2, **(2011)**, pp. 69-80.

[11] H. Weerasinghe and H. Fu, "Preventing Cooperative Black Hole Attacks in Mobile Ad Hoc Networks: Simulation Implementation and Evaluation", International Journal of Software Engineering and Its Applications, vol. 2, no. 3, **(2008)**, pp. 39-54.

[12] B. K. Lee, E. H. Jeong and S. H. Yang, "A SAP(Safe Authentication Protocol) design against a Sybil Attack on VANET", International Conference on Computer and Applications (CCA 2012), Proceedings, Seoul, Korea, **(2012)** March 30-31.

[13] The Network Simulator NS-2, http://www.isi.edu/nsnam/ns.

[14] NAM: Network Animator, http://www.isi.edu/nsnam/nam.

[15] Q. Huang, J. Cukier, H. Kobayashi, B. Liu and J. Zhang, "Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks", WSNA'03 Proceedings of the 2nd ACM International conference on Wireless Sensor Networks and Applications, San Diego, CA, USA, **(2003)** September 19-19.

[16] M. Aydos, T. Yantk and C. K. Koc, "An High-Speed ECC-based Wireless Authentication Protocol on an ARM Microprocessor", The 16th Annual Computer Security Applications Conference, New Orleans, LA, **(2000)** December 11-15.

[17] C. Zhang, R. Lu and X. Lin, "An efficient identity-based batch verification scheme for vehicular sensor networks", IEEE INFOCOM, **(2008)**, pp. 816-824.

Authors

ByungKwan Lee received his B.S. degree from Pusan National University in 1970, the M.S. Degree in Computer Science from Chung-Ang University in 1986 and the ph.D. degree in Computer Science from Chung-Ang University in 1990 in Korea. He has been on the faculty of department of Computer Science and Engineering, Kwan-Dong University, Kang-Won-Do, Korea since 1988. He had been a visiting processor in Saginaw Valley State university, Michigan, USA for two years since 2000. He is a permanent member of the KISS and KIPS. His current research interests are distributed and network management, network security.

EunHee Jeong received her B.S. degree from Kangnung National University in 1991, the M.Eng. degree in Computer Science from Kwandong University in 1998 and the Ph.D. degree in Computer Science from Kwandong University in 2003 in Korea. She has been a professor of department of Regional Economics at Kangwon National University in Korea since 2003, Sept. She is a regular member of the KSII. Her current research interests are Sensor Network, IT security, web programming, and e-commerce.

Ina Jung received her B.Eng. degree from Kwandong National University in 2011, the M.Eng. degree in Computer Science from Kwan-Dong University in 2012. She is currently working towards a doctorate in Computer Science from Kwandong University. Her current research interests are Sensor Network, IT security, and Network security.