ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

Comparison of Different Cryptography Approach for Secure Communication in Vehicular AD-Hoc Network

Kritika Jashnani[1], Prof. Prabhat Sharma[2]

M.Tech Student, Dept. of Electronics&Communication Engineering , OIST Bhopal- (M.P.), India[1]

Asst.Professor, Dept. of Electronics&Communication Engineering , OIST Bhopal- (M.P.), India[2]

ABSTRACT: VEHICULAR ad hoc networks (VANETs) have attracted a lot of attention due to their potential to offer a better driving experience and road safety, as well as many other value added services. Security issues are critical in VANETs because many different forms of attacks against VANETs may emerge due to the use of wireless devices in VANET communications. The basic idea is to allow vehicles to send traffic information to roadside units (RSUs) or other vehicles. Vehicles have to be prevented from some attacks on their privacy and misuse of their private data. For this reason, the security and privacy preservation issues are important prerequisites for VANET. Different cryptography methods are using to make VANET more secure and efficient for practical use. In this paper, we point out reliability of some conventional cryptography scheme for VANET and find an improved scheme that can satisfy the security and privacy desired by vehicles. The cryptography schemes provide the provable security in the random oracle model. In addition, the different scheme needs only a small constant number of pairing and point multiplication computations, independent of the number of messages. We show the efficiency merits, simulation time, different software etc.

KEYWORDS: VANET, RSU, Cryptography, Ad-Hoc

I. INTRODUCTION

VEHICULAR ad hoc networks (VANETs) promise great enhancement to traffic safety and traffic management [1], [2] with wireless vehicle-to-vehicle and vehicle-to-roadside communications. Specifically, enabling nearby vehicles to wirelessly share driving states, VANETs enable various traffic safety applications such as collision avoidance and lane change assistance. In addition, in VANETs, real-time traffic data can be collected from vehicles to improve traffic management. Thus, the potential to improve traffic safety and traffic management will push VANETs to be massively deployed in the future. Furthermore, with free vehicular communications, VANETs provide a handy platform to more cost effective solutions to various value-added applications, e.g., on-road entertainment [3] and automatic survey [4]. Comparatively, existing cellular communications [third-generation (3G) and fourth-generation (4G)] will incur service fees to support such value-added applications. Considering numerous vehicles available in VANETs, one particularly attractive value-added application is for commercial service providers (SPs) to promote their businesses with VANET-based ad dissemination. In addition to being more cost effective than ad dissemination based on cellular communications, VANET-based ad dissemination can easily target ad receivers in specific regions. On the other hand, VANET based ad dissemination is more cost effective and flexible than roadside ad posters, which involve costly human efforts in ad posting and update. However, without pragmatic cost and effect control, arbitrary ad disseminations from various SPs may cause unnecessary distractions to drivers and message storms to VANETs. In addition, the security and privacy issues of ad dissemination also call for thorough investigation. As further discussed in Section II, the existing schemes only, at best, partially tackle the aforementioned challenges. Thus, in this paper, a VANET-based Ambient Ad-Dissemination scheme (VAAD) is proposed to ensure secure ad dissemination with pragmatic cost and effect control. Specifically, VAAD features three major contributions.

1) An incentive-centered architecture is proposed to encourage the SPs to set reasonable cost and effect requirements for ad dissemination.

2) A novel distance-based gradient (DBG) algorithm is proposed to disseminate ads to emulate the ad posting patterns in the physical world and control the cost and effect of ad dissemination.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

3) An efficient, secure, and privacy-preserving incentive cash-in algorithm is proposed to encourage the cooperation of vehicular nodes and support economic value creation. One fundamental security problem in VANETs is message authentication. Achieving message authentication consists of two essential security checks, i.e., an integrity check and identification check. Message authentication must be implemented to allow vehicle users to differentiate reliable information from bogus information and to resist modification attacks and impersonation attacks. An appealing solution to this problem in VANETs is to digitally sign messages before sending them; not only does this allow the receiver to identify the sender, but the signature also prevents the message contents from being modified in transit. Several schemes have been proposed in the literature and can be mainly divided into the following two categories: traditional public-key-infrastructure (PKI)-based digital signature schemes [5], [7] and group signature-based security schemes [2]. In both categories, each message needs to be signed by the sender using an asymmetric algorithm, and its receiver needs to verify the message that is received. Both of these schemes can effectively ensure secure communication while simultaneously protecting user
privacy, but traditional PKI-based schemes may fail to satisfy the stringent time requirements of vehicular communication applications. Particularly as the traffic density increases, a vehicle may become unable to verify the authenticity of the messages sent by its neighbours in a timely manner, which results in message loss and, in turn, an increased risk to public safety.

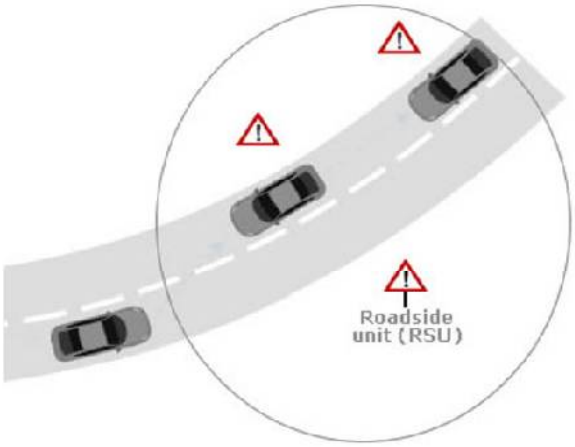

Fig.1 Vehicle-to-roadside communication

II. DIFFERENT CRYPTOGRAPHY SCHEME

A. Identity-based Batch Verification

In this paper, we proposed an efficient identity-based batch verification (IBV) scheme for vehicle-to-infrastructure and inter-vehicle communications in vehicular ad hoc network (VANET). The batch-based verification for multiple message signatures is more efficient than one-by-one single verification when the receiver has to confirm a large number of messages. In particular, the batch verification process of the proposed IBV scheme needs only a constant number of pairing and point multiplication computations, independent of the number of message signatures. Therefore, the batch verification can dramatically decrease the time cost on verifying a large number of message signatures, which can achieve much better scalability. The security analysis shows that the proposed IBV scheme not only achieves the privacy preserving desired by vehicles and the traceability required by the trust authority, but also satisfies the security issues such as message authentication, integrity, non-repudiation, unlink ability and replaying resistance. We also prove that the proposed IBV scheme is secure against existential forgery in the random oracle model under the computational Diffie-Hellman problem. In the performance analysis, we have evaluated the proposed IBV scheme with other batch verification schemes in terms of computation delay and transmission overhead. Moreover, we verify the efficiency and practicality of the proposed scheme by the simulation analysis. Simulation results show that both the average message delay and message loss rate of the proposed IBV scheme are less than those of the existing schemes.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

In the future work, we will continue our efforts to enhance the features of IBV scheme for VANET, such as recognizing illegal signatures. When attackers send some invalid messages, the batch verification may lose its efficacy. This problem commonly accompanies other batch-based verification schemes [1]. Therefore, thwarting the invalid signature problem is a challenging and a topic for study in our future research.

B. Proxy Vehicles

The PBAS makes use of vehicles' computational capacity to reduce the burden of RSUs, where the proxy vehicles can authenticate multiple messages from the other vehicles. The PBAS also provides RSUs with a systematic and independent mechanism to verify the messages from the proxy vehicles.

In addition, the PBAS can negotiate a session key with every other vehicle for the confidentiality of sensitive information. The evaluation model of the PBAS showed that the PBAS offers fault tolerance, which enables the scheme to continue operating properly even if a small number of proxy vehicles are compromised in VANETs. Moreover, we analyzed and compared the performance of the PBAS with the other authentication schemes in terms of their computation and transmission overheads. We also used simulations to verify the efficiency of the PBAS in realistic environments, showing that the PBAS is a promising security scheme for efficient VANET authentication. In this paper, on the PBAS, we focused on a cryptography algorithm under the assumption that any vehicle having completed system initialization can act as a proxy vehicle. However, it is crucial to make sure that these vehicles have incentives to serve for the others under the condition of efficient message delivery. In the future, we will exploit the game theory to study the incentive mechanism. The redundant authentication is another issue, in which different proxy vehicles may work on
the same message. To minimize the redundant authentication events, we should design a selection strategy that combines extra computation resource utilization optimization and redundant authentication reduction.

C. ECC, RSA, ECDSA

RSA, Elliptic Curve Cryptography (ECC) and Elliptic Curve Digital Signature Algorithm (ECDSA) are three commonly adopted asymmetric algorithms. In RSA, the public key contains a large non-prime number, the RSA modulus, which is chosen as the product of two large primes. The security of RSA is based on the difficulty of the integer factorization problem. The size of an RSA key refers to the bit-length of the RSA modulus [7]. Due to the efficiency of RSA, the generation of key pairs and the public-key based pseudonym in the current public key in [7] was implemented by an RSA algorithm. ECC is an approach based on the algebraic structure of elliptic curves over finite fields [7]. The entire security of ECC depends on the ability to compute a point multiplication and the inability to compute the multiplication given the original and product points. ECC algorithm has the advantage of providing much shorter key sizes and system parameters than RSA. ECDSA is the elliptic curve analog of the digital signature algorithm (DSA) [64]. IEEE 1609.2 [7] proposed the use of ECDSA to verify messages.

D. Blow fish

Blowfish: Blowfish is a symmetric-key block cipher, de-signed in 1993 by Bruce Schneier. Blowfish provides a good encryption rate in software. It is a fast, compact, and simple block encryption algorithm with variable length key allowing a tradeoff between speed and security. Blowfish is unpatented and license-free, and is available free for all applications. Blowfish is known to be susceptible to attacks on reflectively weak keys [7]. This means Blowfish users must carefully select keys as there is a class of keys known to be weak. Though it suffers from weak keys problem, but no attack is pendent S-boxes and sub keys, generated using cipher itself, makes analysis very difficult and provided key is large enough, so brute-force key search is not practical, especially given the high key schedule cost. It is invulnerable against differential related-key attacks.

E. Camellia

Camellia was jointly developed by Nippon Tele-graph and Telephone Corporation and Mitsubishi Electric Corporation in 2000 [11,12]. It possesses the security level and processing capability equivalent to AES. Camellia is character-ized by its suitability for both software and hardware imple-mentations on common 32-bit processors as well as 8-bit pro-

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

cessors (e.g., smart cards, cryptographic hardware, and em-bedded systems). Camellia's application in IPsec is described in RFC 4312 and application of OpenPGP in RFC 5581.It has high level of security. The design goals of Camellia are: High level of security and efficiency on multiple platforms. The fea-tures of Camellia are outlined as follows:
- The Feistel structure with either 18 rounds (when using 128-bit keys) or 24 rounds (when using 192 or 256-bit keys)
- 128-bit input/output data block size
- 128, 192, and 256-bit key sizes
- Using 8x8 S-boxes.

F. CAST-128

The algorithm was created in 1996 by Carlisle Adams and Stafford Tavares using the CAST design proce-dure. CAST-128 (described in RFC-2144 document [13]) is a popular 64-bit block cipher allowing key sizes up to 128 bits. The name CAST stands for Carlisle Adams and Stafford Tavares, the inventors of CAST. It is used in some applications as the default cipher in some versions of GPG and PGP. It has also been approved for Canadian government use by the Communications Security Establishment. One of the positive characteristics in this method is inmunity against differential and linear cryptanalysis attacks; standard cipher algorithm on last versions of PGP [17]. The features of CAST-128 are:
- The Feistel structure with either 12 or 16 round.
- 64-bit input/output data block size
- A key size between 40 to 128 bits (but only in 8-bit in-crements). The full 16 rounds are used when the key size is longer than 80 bits.
- Using large 8×32-bit S-boxes.

III. COMPARISON CHART RESULT

Methods	Simulation tool	Simulation time	Packet size	Wireless protocol
Id-based	NS-2	80s	67 bytes	802.11a
PBAS	NS-2	100s	70 bytes	802.11p
ECC, RSA, ECDSA	C Ubuntu 12.04	8s	20, 128 bytes	802.11p
Blow fish	C Ubuntu 12.04	80s-100s	56 bytes	802.11a
Camellia	C Ubuntu 12.04	80s-100s	32 bytes	802.11a
CAST-128	C Ubuntu 12.04	80s-100s	16 bytes	802.11a

IV. CONCLUSION

Encryption algorithm plays very important role in Communication security over VANET. Our research work surveyed over the performance of existing encryption techniques like ID, PBAS, ECC, RSA, ECDSA, Blow fish, Camellia, Cast-128 algorithms. Based on the text files used and the experimental result it was concluded that ECC, algorithm consumes least encryption and RSA consume longest encryption time. We also observed that Decryption of RSA algorithm is better than other algorithms. From the simulation result, we evaluated that ECC, RSA, ECDSA algorithm is much better than DES algorithm. Our future work will focus on develop novel cryptography algorithm which is best in terms of simulation time, using software, buffer size, etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2016

REFERENCES

[1] Shiang-Feng Tzeng, Shi-Jinn Horng, Tianrui Li, Xian Wang, Po-Hsian Huang, and Muhmmad Khurram Khan "Enhancing Security and Privacy for Identity-based Batch Verification Scheme in VANET 10.1109/TVT.2015.2406877, IEEE Transactions on Vehicular Technology.2015
[2] Yiliang Liu, Liangmin Wang, Member, IEEE, and Hsiao-Hwa Chen, Fellow, IEEE" Message Authentication Using Proxy Vehicles in Vehicular Ad Hoc Networks" IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 64, NO. 8, AUGUST 2015
[3] IEEE TRANSACTIONS ON INTELLIGENT TRANSPORTATION SYSTEMS, VOL. 16, NO. 6, DECEMBER 2015 2985 A Security and Privacy Review of VANETs Fengzhong Qu, Senior Member, IEEE, Zhihui Wu, Fei-Yue Wang, Fellow, IEEE, and Woong Cho, Member, IEEE
[4] IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 8, NO. 11, NOVEMBER 2013 b-SPECS+: Batch Verification for Secure Pseudonymous Authentication in VANET Shi-Jinn Horng, Shiang-Feng Tzeng, Yi Pan, Pingzhi Fan, Senior Member, IEEE, XianWang, Tianrui Li, Senior Member, IEEE, and Muhammad Khurram Khan
[5] An Identity-Based Security System for User Privacy in Vehicular Ad Hoc Networks Jinyuan Sun, Chi Zhang, Yanchao Zhang, and Yuguang Fang, Fellow, IEEE IEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 21, NO. 9, SEPTEMBER 2010
[6] EMAP: Expedite Message Authentication Protocol for Vehicular Ad Hoc Networks Albert Wasef and Xuemin (Sherman) Shen, IEEE, Fellow IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 1, JANUARY 2013
[7] International Journal of Scientific & Engineering Research, Volume 5, Issue 2, February-2014 911 ISSN 2229-5518 IJSER © 2014 http://www.ijser.org Performance Analysis of Cryptography Methods for Secure Message Exchanging in VANET M. Alimohammadi, and A. A. Pouyan
[8] R. Lu, Doctoral dissertation, , University of Waterloo, 2012. Security and Privacy Preservation in Vehicu-lar Social Networks

[9] C. Zhang, Doctoral dissertation, , University of Waterloo, 2010. On Achieving Secure Message Authentica-tion for Vehicular Communications

[10] 1TT. W. Chim, S. M. Yiu, L. C. K. Hui, & V. O. K. Li, Grouping-enabled and privacy-enhancing.0T1T 0TInformation Systems Security1T,0T1T vol. 0T7, no. 1T1, pp. 60-96, 2011.1T

[11] S., Qi, Y. Chang, H. Zhu, J. Zhao, & X. Shen, Footprint: Detecting Sybil Attacks in Urban Vehicular Networks. Parallel and Distributed Systems, IEEE Transactions on, vol. 23, no. 6, pp. 1103-1114, 2012.

[12] S. Park, B. Aslam, D. Turgut, & C. C. Zou, Defense against Sybil at-tack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. Security and Communication Net-works, vol. 6, no. 4, pp. 523–538, 2013.