Volume 2, Issue 2, February 2012 ISSN: 2277 128X

www.ijarcsse.com

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

User Privacy ISP Using VANET

Er.Krishna Ganesh S.M[1]
Department of Computer Science and Engineering
St. Joseph College of Engineering and Technology

Er.Ashok Kumar .T[2]
Department of Computer Science and Engineering
St. Joseph College of Engineering and Technology

***Abstract*—Vehicular ad hoc network (VANET) can offer various services and benefits to users and thus deserves deployment effort. Attacking and misusing such network could cause destructive consequences. It is therefore necessary to integrate security requirements into the design of VANETs and defend VANET systems against misbehaviour, in order to ensure correct and smooth operations of the network. In this paper, we propose a user privacy ISP(Independent Security Pattern) using VANETs to achieve privacy desired by vehicles and traceability required by law enforcement authorities, in addition to satisfying fundamental security requirements including authentication, nonrepudiation, message integrity, and confidentiality. Moreover, we propose a User privacy ISPpreserving defense technique for network authorities to handle misbehaviour in VANET access, considering the challenge that privacy provides avenue for misbehaviour. The proposed system employs an identity-based cryptosystem where certificates are not needed for authentication. We show the fulfilment and feasibility of our system with respect to the security goals and efficiency.**

Keywords*— Privacy, traceability, pseudonym, misbehavior, revocation, identity-based cryptography, vehicular ad hoc network,ISP(Independent Security Pattern)

I. INTRODUCTION

A Vehicular Ad-Hoc Network, or VANET, is a technology that uses moving cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes. With the Internet becoming an increasingly significant part of our lives, the dream of a Wi-Fi-enabled city is becoming closer and closer to reality. One of the hindrances to that dream, however, is the high router requirement; for wireless internet to blanket a city, thousands of wireless routers must be strategically placed to ensure constant coverage. Since this is a process that can become quite complicated and costly, researchers at UCLA began looking for an existing technology to which routers could be attached or involved. Since Los Angeles is a city already plagued with traffic problems, the UCLA Vehicular Network Lab was established to study the possibility of wirelessly connected automobiles. The Vehicular Ad-Hoc Network, or VANET, is a technology that uses moves cars as nodes in a network to create a mobile network. VANET turns every participating car into a wireless router or node, allowing cars approximately 100 to 300 metres of each other to connect and, in turn, create a network with a wide range. As cars fall out of the signal range and drop out of the network, other cars can join in, connecting vehicles to one another so that a mobile Internet is created. It is estimated that the first systems that will integrate this technology are police and fire vehicles to communicate with each other for safety purposes

II. TECHNOLOGY OF VANETS

In VANET, or Intelligent Vehicular Ad-Hoc Networking, defines an Intelligent way of using Vehicular Networking. In VANET integrates on multiple ad-hoc networking technologies such as WiFi IEEE 802.11 b/g, WiMAX IEEE 802.16, Bluetooth, IRA, ZigBee for easy, accurate, effective and simple communication between vehicles on dynamic mobility. Effective measures such as media communication between vehicles can be enabled as well methods to track the automotive vehicles is also preferred.In VANET helps in defining safety measures in vehicles, streaming communication between vehicles, infotainment and telematics.Vehicular Ad-hoc Networks are expected to implement variety of wireless technologies such as Dedicated Short Range Communications (DSRC) which is a type of WiFi. Other candidate wireless technologies are Cellular, Satellite, and WiMAX. Vehicular Ad-hoc Networks can be viewed as component of the Intelligent Transportation Systems (ITS).Vehicular Networks are an envision of the Intelligent Transportation Systems (ITS). Vehicles communicate with each other via Inter-Vehicle Communication (IVC) as well as with roadside base stations via Roadside-to-Vehicle Communication (RVC). The optimal goal is that vehicular networks will contribute to safer and more efficient roads in the future by providing timely information to drivers and concerned authorities.

III. EXISTING SYSTEM

There is a large body of research work related to the security and privacy in VANETs. The most related works are on the design of privacy-preserving schemes. The privacy issue by proposing a pseudonym-based approach using anonymous public keys and the public key infrastructure (PKI), where the public key certificate is needed, giving rise to extra communication and storage overhead. The three credential revocation protocols tailored for VANETs, namely RTPD, *RC*2*RL*, and DRP, considering that the certificate revocation list (CRL) needs to be distributed across the entire network in a timely manner.

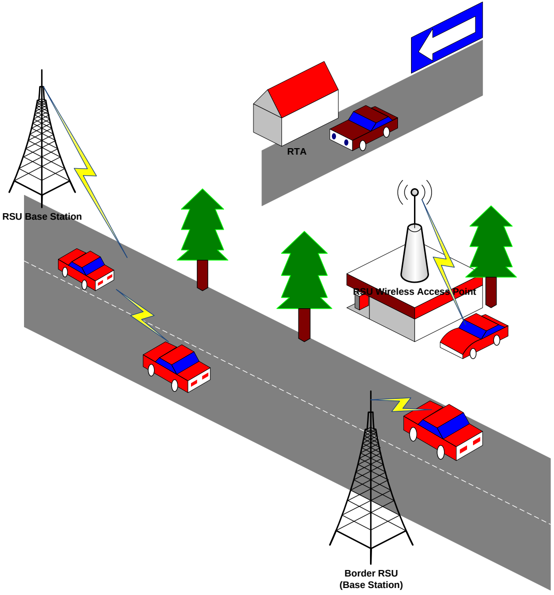


Fig: VANET System

The above figure shows a structure of a VANET system. All the three protocols seem to work well under conventional public key infrastructure (PKI). However, the authors also proposed to use frequently updated anonymous public keys to fulfill users' requirement on identity and location privacy. If this privacy preserving technique is used in conjunction with *RC*2*RL* and DRP, the CRL produced by the trusted authority will become huge in size, rendering the revocation protocols highly inefficient. A lightweight symmetric-key based security scheme for balancing auditability and privacy in VANETs is proposed in. It bears the drawback that peer vehicles authenticate each other via a base station, which is unsuitable for inter-vehicle communications. An identity-based (ID based) ring signature scheme to achieve signer ambiguity and hence fulfil the privacy requirement in VANET applications.The disadvantage of the ring signature scheme in the context of VANET applications, is the unconditional privacy, resulting in the traceability requirement unattainable. Group signature based schemes are proposed in, where signer privacy is conditional on the group manager. As a result, all these schemes have the problem of identity escrow, as a group manager who possesses the group master key can arbitrarily reveal the identity of any group member. In addition, due to the limitation of group formation in VANETs (e.g., too few cars in the vicinity to establish the group), the group-based schemes may not be applied appropriately. The election of group leader will sometimes encounter difficulties since a trusted entity cannot be found amongst peer vehicles.However, their framework is limited by the strong dependence on the frastructure for short-lived pseudonym generation, which renders the signaling overhead overwhelming. The proposed nonrepudiation scheme enables a single authority to retrieve the identity which may raise the concern on potential abuse. Schemes leveraging pseudonyms in VANETs can also be found in with the revocation feasible in limited settings, and in where the certificate authority maintains mapping from an identity to the set of vehicle-generated pseudonyms. There are also a number of defense techniques against misbehavior in VANET literature besides those in.

An indirect approach via the aid of infrastructure is used. The TA distributes the CRL to the infrastructure points which then take over the TA's responsibility to execute the revocation protocol. The advantage of this approach is that vehicles never need to download the entire CRL. Unfortunately, the conditional anonymity claimed and only applies to amongst peer vehicles, under the assumption that the infrastructure points are trusted. The infrastructure points can reveal the identity of any vehicle at any time even if the vehicle is honest. The scheme leverages a single TA to recover the identity of a (possibly honest) vehicle, where revocation issues are not discussed.

III-A.ID-BASED CRYPTOGRAPHY (IBC)

Identity-based or ID-based cryptosystem allows the public key of an entity to be derived from its public entity information such as name, email address, etc, which avoids the use of certificates for public key verification in the conventional PKI. Boneh and Franklin introduced the first functional and efficient ID-based encryption scheme based on bilinear pairings on elliptic curves. Specifically, let $G1$ and $G2$ be an additive group and a multiplicative group, respectively, of the same prime order *q*.IBC schemes are used mainly for encryption, authentication, and non-repudiation in our VANET system. Compared to the conventional PKI (public key infrastructure), IBC infrastructure avoids the use of certificates for public key verification and the exchange of public keys (and associated certificates), greatly improving the computation and communication efficiency.

III-B. THRESHOLD SCHEMES BASED ON SECRET SHARING

Threshold schemes are used as cryptographic means to distribute secret information to multiple entities to eliminate power centralization and a single point of failure.

IV. PROPOSED SYSTEM

The Proposed User privacy ISP using (VANETs) are receiving increasing attentions from academia and deployment efforts from industry, due to the various applications and potential tremendous benefits they offer for future VANET users. Safety information exchange enables life critical application, such as the alerting functionality during intersection traversing and lane merging, and thus plays a key role in VANET applications . value-added services can enhance drivers' traveling experience by providing convenient Internet access, navigation, toll payment services, etc. more other applications are also possible including different warning messages for congestion avoidance, detour notification, road conditions (e.g., slippery), etc., and alarm signals disseminated by emergency vehicles (e.g., ambulance) for road clearance. The attractive features of VANETs inevitably incur higher risks if such networks do not take security into account prior to deployment. For instance, if the safety messages are modified, discarded, or delayed either intentionally or due to hardware malfunctioning, serious consequences such as injuries and even deaths may occur. This necessitates and urges the development of a functional, reliable and efficient security architecture before all other implementation aspects of VANETs. Fundamentally, VANET security design should guarantee authentication, non-repudiation, integrity, and in some specific application scenarios, confidentiality, to protect the network against attackers. Besides the fundamental security requirements, sensitive information such as identity and location privacy should be preserved from the vehicle owner's perspective, against unlawful tracing and user profiling, since otherwise it is difficult to attract vehicles to join the network. On the contrary, traceability is required where the identity information need be revealed by law enforcement authorities for liability issues, once accidents or crimes occur. In addition, privilege revocation is required by network authorities (e.g., network administrator) once misbehavior is detected during network access. It is less difficult to prevent misbehavior of unauthorized users (i.e., outsiders) since legitimate users and roadside units (RSUs) can simply disregard communication requests from outsiders by means of authentication. Nevertheless, misbehavior of legitimate users of VANETs (i.e., insiders) is more difficult and complex to prevent, the reason being that insiders possess credentials issued by the authority to perform authentication with peer vehicles or RSUs who can be easily tricked into trusting the insiders. Consequently, the insiders' misbehavior will have much larger impact on the network and will be the focus of this paper. Our proposed system in this paper and many recent proposals on VANET security, provide the option of using anonymous credentials in authentication, rendering it even more complex to handle misbehavior in VANETs, since the user identity is hidden and cannot be linked arbitrarily which curbs the punishment of misbehaving users.

III. SYSTEM SET UP

This procedure is executed by the RTA for initial VANET system setup including domain parameter publication, public/private key assignment for entities in the system to perform desired tasks, and database creation for storing necessary records (i.e., the pseudonym lookup table PLT).

A. PSEUDONYM GENERATION AND AUTHENTICATION FOR PRIVACY:

RTA and border RSUs execute this procedure to assign pseudonym/private key pairs to both vehicles traveling in their home domain and vehicles from other RTAs' domains, so that these vehicles are able to authenticate with RSUs and other vehicles to obtain services and useful messages.

B. THRESHOLD SIGNATURE FOR NONFRAMEABILITY

This procedure is invoked by LEAs to share the secret information for recovering a guilty vehicle's identity. Meanwhile, it prevents corrupted authorities from gathering full power to accuse an innocent vehicle. The functional component of this procedure is the threshold.

C. THRESHOLD-AUTHENTICATION-BASED DEFENSE:

Designed for the network authorities, this procedure is used to revoke a misbehaving vehicle's credential, refraining the vehicle from further disrupting system operations. As the core of this procedure, the threshold authentication technique provides a mechanism to allow certain types of misbehavior that should not result in revocation. For instance, the misbehavior may be caused by malfunctioning hardware and thus is incidental. These types of misbehavior share a commonfeature, i.e., their occurrence or frequency is low, specifically, lower than a predetermined threshold. Threshold authentication-based defense further consists of six sub-procedures:

E. Membership registration

RSUs and vehicle users register with the RTA to use VANETs. Upon successful registration, a member public/private key pair (mpk; msk) is issued to each RSU and vehicles. The RTA associates the member's credential with the issued public key and includes this pair of information into a credential list IDlist.

F. Access group setup:

RSUs and vehicles setup their own access groups, the member of which is granted privilege to communicate with the access group owner. The group owner adds members to the group and updates related public information. Each added member obtains an access key mak for the group.

G. Access group revoking:

The access group owner revokes the granted privilege when deciding to stop communications with a member, due to some decision criteria for misbehavior. The access group owner removes the member from the access group and updates related public information.

H. Threshold authentication:

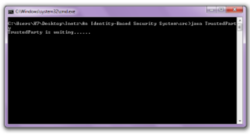
This procedure is executed between an RSU and a vehicle, or between peer vehicles. We call the authenticator in this procedure Alice who announces the threshold k possibly different for each user being authenticated. The authentication succeeds if and only if the following conditions are met simultaneously: the user Bob authenticating with Alice is a registered member of the VANET system, Bob is a legitimate member of Alice's access group (if Alice is an access group owner) whose member privilege has not been revoked, and the authentication threshold has not been exceeded. Alice records the authentication transcripts in AUTHlog:

I. TracinG

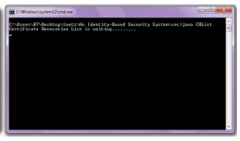
This procedure is used by Alice to trace a misbehaving member Mn who attempts to authenticate more than k times. Alice relies on the AUTHlog and public information, and obtains Mn's credential n as the procedure output which is reported to the RTA.

J. Revocation/recovery:

Upon receiving the complaints from other entities in the system as the output of Tracing, the RTA decides if the misbehaving member's credential needs to be revoked. The RTA then performs the identity recovery by looking up the same pseudonym lookup table PLT (cf. System setup above) which also records the correspondence between the credential n and identity IDn. Note that for the ease of presentation, we assume the RTAs to act as network authorities for the defense scheme in this paper. In reality, when the roles of RTA and network authority are separate, the network authority can simply take charge as the RTA in the above subprocedures. Nonetheless, in the execution of Revocation/recovery, the network authority needs to establish trust with or be delegated by the RTA in order to access the PLT. When we mention network authorities in what follows, we implicitly refer to RTAs in the network authority role

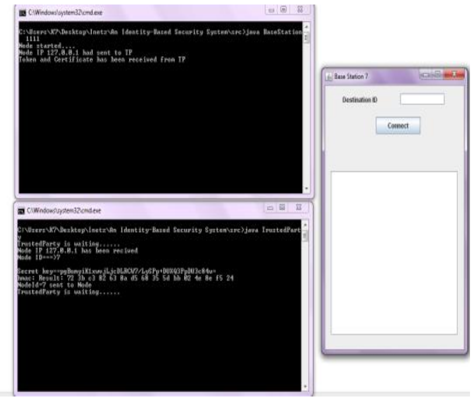


```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java TrustedPart
y
TrustedParty is waiting......
```



```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java CRList
Certificate Revocation List is waiting.........
_
```

Fig: Trusted Party is waiting Fig: Certificate Revocation list is waiting

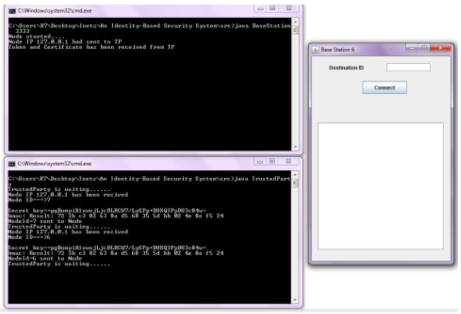


```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java BaseStation
  1111
Node started....
Node IP 127.0.0.1 had sent to TP
Token and Certificate has been received from TP
```

```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java TrustedPart
y
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>7

Secret key==pgBunyiK1xwvjLjcDLRCW7/LySPp+DUXQ3PpDU3c84w=
hmac: Result: 72 3b c3 82 63 8a d5 68 35 5d bb 02 4e 8e f5 24
NodeId=7 sent to Node
TrustedParty is waiting......
```

Fig: Creating a base station



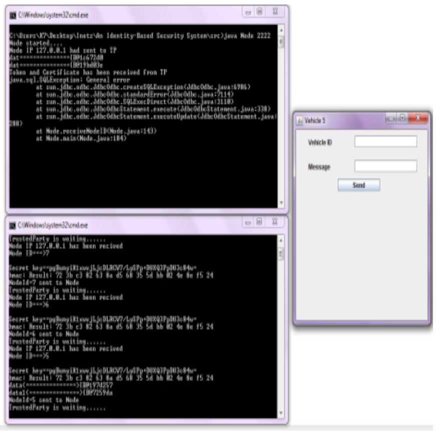
```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java BaseStation
  3333
Node started....
Node IP 127.0.0.1 had sent to TP
Token and Certificate has been received from TP
```

```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java TrustedPart
y
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>7

Secret key==pgBunyiK1xwvjLjcDLRCW7/LySPp+DUXQ3PpDU3c84w=
hmac: Result: 72 3b c3 82 63 8a d5 68 35 5d bb 02 4e 8e f5 24
NodeId=7 sent to Node
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>6

Secret key==pgBunyiK1xwvjLjcDLRCW7/LySPp+DUXQ3PpDU3c84w=
hmac: Result: 72 3b c3 82 63 8a d5 68 35 5d bb 02 4e 8e f5 24
NodeId=6 sent to Node
TrustedParty is waiting......
```

Fig: Creating another base station node



```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java Node 2222
Node started....
Node IP 127.0.0.1 had sent to TP
dat===============[B@1c672d0
dat===============[B@19bd03e
Token and Certificate has been received from TP
java.sql.SQLException: General error
        at sun.jdbc.odbc.JdbcOdbc.createSQLException(JdbcOdbc.java:6986)
        at sun.jdbc.odbc.JdbcOdbc.standardError(JdbcOdbc.java:7114)
        at sun.jdbc.odbc.JdbcOdbc.SQLExecDirect(JdbcOdbc.java:3110)
        at sun.jdbc.odbc.JdbcOdbcStatement.execute(JdbcOdbcStatement.java:338)
        at sun.jdbc.odbc.JdbcOdbcStatement.executeUpdate(JdbcOdbcStatement.java:
288)
        at Node.receiveNodeID(Node.java:143)
        at Node.main(Node.java:104)
```

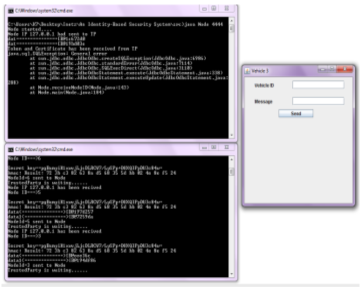
```
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>7

Secret key==pgBumyiXiuwjLjcDLRCV7/LyGPp+D0XQJPpDU3c84w=
hmac: Result: 72 3b c3 02 63 8a d5 68 35 5d bb 02 4e 8e f5 24
NodeId=7 sent to Node
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>6

Secret key==pgBumyiXiuwjLjcDLRCV7/LyGPp+D0XQJPpDU3c84w=
hmac: Result: 72 3b c3 02 63 8a d5 68 35 5d bb 02 4e 8e f5 24
NodeId=6 sent to Node
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>5

Secret key==pgBumyiXiuwjLjcDLRCV7/LyGPp+D0XQJPpDU3c84w=
hmac: Result: 72 3b c3 02 63 8a d5 68 35 5d bb 02 4e 8e f5 24
data(===============)[B@197d257
data1(===============)[B@7259da
NodeId=5 sent to Node
TrustedParty is waiting......
```

Fig: Creating a vehicle node



```
C:\Users\K7\Desktop\Inetz\An Identity-Based Security System\src>java Node 4444
Node started....
Node IP 127.0.0.1 had sent to TP
dat===============[B@1c672d0
dat===============[B@19bd03e
Token and Certificate has been received from TP
java.sql.SQLException: General error
        at sun.jdbc.odbc.JdbcOdbc.createSQLException(JdbcOdbc.java:6986)
        at sun.jdbc.odbc.JdbcOdbc.standardError(JdbcOdbc.java:7114)
        at sun.jdbc.odbc.JdbcOdbc.SQLExecDirect(JdbcOdbc.java:3110)
        at sun.jdbc.odbc.JdbcOdbcStatement.execute(JdbcOdbcStatement.java:338)
        at sun.jdbc.odbc.JdbcOdbcStatement.executeUpdate(JdbcOdbcStatement.java:
288)
        at Node.receiveNodeID(Node.java:143)
        at Node.main(Node.java:104)
```

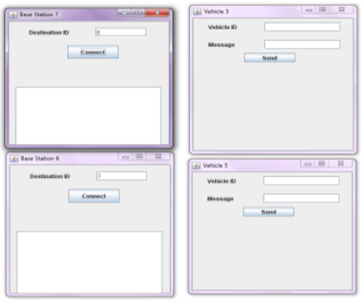
```
Node ID===>6

Secret key==pgBumyiXiuwjLjcDLRCV7/LyGPp+D0XQJPpDU3c84w=
hmac: Result: 72 3b c3 02 63 8a d5 68 35 5d bb 02 4e 8e f5 24
NodeId=6 sent to Node
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>5

Secret key==pgBumyiXiuwjLjcDLRCV7/LyGPp+D0XQJPpDU3c84w=
hmac: Result: 72 3b c3 02 63 8a d5 68 35 5d bb 02 4e 8e f5 24
data(===============)[B@197d257
data1(===============)[B@7259da
NodeId=5 sent to Node
TrustedParty is waiting......
Node IP 127.0.0.1 has been recived
Node ID===>3

Secret key==pgBumyiXiuwjLjcDLRCV7/LyGPp+D0XQJPpDU3c84w=
hmac: Result: 72 3b c3 02 63 8a d5 68 35 5d bb 02 4e 8e f5 24
data(===============)[B@eee36c
data1(===============)[B@194df86
NodeId=3 sent to Node
TrustedParty is waiting......
```

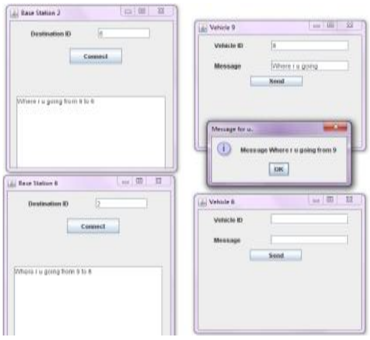
Fig: Creating another vehicle node



Base Station 7 — Destination ID: 6

Base Station 6 — Destination ID: 7

Fig: Establishing communication between base stations



Base Station 2 — Destination ID: 6

Where r u going from 9 to 6

Vehicle 9 — Vehicle ID: 6; Message: Where r u going

Message for u..

Message Where r u going from 9

Base Station 6 — Destination ID: 2

Where r u going from 9 to 6

Fig: Secured Communication

IV. CONCLUSIONS

The proposed User Security ISP(Internet Security Pattern) using VANET mainly achievies privacy, traceability, nonframeability, andprivacypreserving defense against misbehavior. These functionalities are realized by the pseudonym-based technique, the threshold signature, and the threshold authentication based defense scheme. The ID-based cryptosystem facilitates us to design communication and storage efficient schemes. Through security and efficiency analysis, our system is shown to satisfy the predefined security objectives and desirableefficiencies. Our future work consists of simulating the proposed security system and experimenting it in real VANET settings.

ACKNOWLEDGMENT

First of all we thank the almighty for giving us the knowledge and courage to complete the research work successfully. We express our gratitude to our respected Rev.Fr.Dr.Arulraj Founder, DMI Group of institutions, East Africa and India, Dr.T.X.A.Ananth, Director(International Operations), DMI group of institutions, East Africa and India,Mr.Ignatius Herman, Director(Academic),DMI group of institutions, East Africa and India and Dr.V.KrishnanPh.D,Principal,DMI.St.Joseph College of Engg & Technology, Tanzania for allowing us to do the research work internally. Also we acknowledge the support provided by Rev.Sr.Fatima Mary, Vice Principal (Administration), DMI.St.Joseph College of Engg & Technology, Tanzania and Mr.N.Ressel Raj, Vice Principal (Academic), DMI.St.Joseph College of Engg & Technology, Tanzania. We thank our friends and collegues for their support and encouragement.

REFERENCES

[1]. L. Nguyen and R. Safavi-Naini, “Dynamic K-Times Anonymous Authentication,” Proc. Applied Cryptography and Network Security Conf., vol. 3531, pp. 318-333, 2005.

[2]. M. Raya, P. Papadimitratos, I. Aad, D. Jungels, and J.-P. Hubaux, “Eviction of Misbehaving and Faulty Nodes in Vehicular Networks,” IEEE J. Selected Areas Comm., vol. 25, no. 8, pp. 1557-1568, Oct. 2007.

[3]. C. Gamage, B. Gras, B. Crispo, and A.S. Tanenbaum, “An Identity- Based Ring Signature Scheme with Enhanced Privacy,” Proc. Second Int’l Conf. Security and Privacy in Comm. Networks (SecureComm ’06), Aug. 2006.

[4]. R. Lu, X. Lin, H. Zhu, P.-H. Ho, and X. Shen, “ECPP: Efficient Conditional Privacy Preservation Protocol for Secure Vehicular Communications,” Proc. IEEE INFOCOM, Apr. 2008.

[5]. A. Studer, E. Shi, F. Bai, and A. Perrig, “TACKing Together Efficient Authentication, Revocation, and Privacy in VANETs,” Proc. Sixth Ann. IEEE SECON Conf. (SECON ’09), 2009.

[6]. K. Sampigethaya, L. Huang, M. Li, R. Poovendran, K. Matsuura, and K. Sezaki, “Caravan: Providing Location Privacy for Vanet,” Proc. Embedded Security in Cars (ESCAR), 2005.

[7]. P. Kamat, A. Baliga, and W. Trappe, “An Identity-Based Security Framework for VANETs,” Proc. Third ACM Int’l Workshop

Vehicular Ad Hoc Networks (VANET '06), pp. 94-95, Sept. 2006.

[8]. P. Kamat, A. Baliga, and W. Trappe, "Secure, Pseudonymous, and Auditable Communication in Vehicular Ad Hoc Networks," J. Security and Comm. Networks, vol. 1, no. 3, pp. 233-244, June 2008.

[9]. J. Sun and Y. Fang, "Defense Against Misbehavior in Anonymous Vehicular Ad Hoc Networks," Ad Hoc Networks, vol. 7, no. 8, pp. 1515-1525, Nov. 2009.

[10]. G.M. Bertoni, L. Chen, P. Fragneto, K.A. Harrison, and G. Pelosi,"Computing Tate Pairing on Smartcards," http://www.st.com/stonline/products/families/smartcard/ches2005_v4.pdf, 2005

THE AUTHORS

Mr S.M.KrishnaGanesh has completedMasters of Technology Degreein ComputerScienceand Engineering at Kalasalingam University in the year 2009, Tamil Nadu,India.He is currently working as Lecturer in St. Joseph College of engineering and Technology,Dar Es Salaam, Tanzania, East Africa He has guided more than 20 projects to final year B.E/B.Tech students and good industry and teaching experience.His areas of interests are Image Processing, Computer Networks,Neural networks and Bioinformatics.

Mr T.Ashok Kumarhas completedMasters of Engineering Degree in Computer Science and Engineering at P.S.R. Engineering College, in the year 2010, Tamil Nadu, India. He is currently working as Lecturer in St. Joseph College of engineering and Technology, Dar Es Salaam, Tanzania, East Africa. He has guided more than 10 projects to final year B.E/B.Tech students and good teaching experience.His areas of interest are Computer Networks, Image Processing.