International Journal of Applied Engineering Research
ISSN 0973-4562 Volume 10, Number 12 (2015) pp. 30573-30588
© Research India Publications
http://www.ripublication.com

An Anomaly Intrusion Detection With Group Signature Based Authentication In VANET

[1]Mr.A.M.Arul Raj, [2]Dr.E.R.Naganathan
[1]Research Scholar,Department of Computer Science
Hindustan University, Chennai.
arulphd74@gmail.com
[2]Professor, Department of Computer Science
Hindustan University, Chennai.
naganathan@hindustanuniv.ac.in

Abstract

In VANET, providing the authentication is a critical problem. To overcome this in this paper, we proposed an Anomaly Based Intrusion Detection with Group Signature Based Authentication technique for VANET. A trusted set of nodes (TN) are found based on the outcome of intrusion detection. Anomaly Detection scheme based on Bayesian classification is applied for intrusion detection. Then audit data related to new system activities is evaluated to detect deviations between the current and the reference behaviors. New pragmatic data is compared to the reference model by means of a Bayesian classification and cluster pertinence evaluations, if there is a difference then intrusion is detected if the both data are matched then this node is added to set of trusted nodes. The trusted authority (TA) issues digital certificates for vehicles and RSUs and maintains a Certificate Revocation List (CRL) containing the certificates of revoked vehicles. The RSU assigns a group signature to TN for authentication.

Introduction

Vehicular Ad-Hoc Network (VANET)

A special class of Mobile Ad-Hoc Networks (MANETs) is vehicular ad-hoc network (VANET) in which, nodes self-organize and self-manage information in a distributed fashion [1]. A vehicular ad-hoc network (VANET) is a type of network which is formed by combination of vehicles and infrastructure points [2]. Infrastructure points are called road side units (RSUs). RSUs are positioned at definite space on the road, alike an access point in conventional wireless ad hoc networks for providing compulsory infrastructure support for network setup and communications. There is no need of fixed infrastructure, like base station or, mobile switching center in VANET [3]. In vehicular ad-hoc network (VANET) the communication can either be among vehicle (vehicle-to-vehicle) or between vehicle and infrastructure (vehicle-to-infrastructure) [1] [2] [3] [4].

Attacks on VANET

Impersonation attack

An impersonation attack is a type of attack in which an adversary effectively assumes the identity of one of the genuine parties in a system or in a communications protocol. In Impersonation attack the attacker steals other entity's credential and performs as another entity. As a result, some warnings sent to a particular entity would be sent to an undesired one [6].

Sybil Attack

The attacker sends numerous messages to other vehicles and each message enclose different fabricated source identity (ID) in Sybil attack. It presents misapprehension to other vehicle by sending some off beam messages like traffic jam message. [1] [7]

Authentication In VANET

Authentication can be considered as the first line of defense against intruders. It is the verification of a user's identity prior to granting access to the network. [5] Authentication is the ability to distinguish between these sources malicious and genuine sources for messages in VANETs [8]. In VANET, authentication is a procedure, which is use to verify the approved identity of a vehicle by a system, while the secret private information is not disclosed when that exposé would cause either mortification or suffering to the vehicle of sensible sensitivities [6]. There are two techniques of authentication, which are: 1) group signature schemes and 2) pseudonyms. In signature scheme, a private key is given to each user, with which it signs the message. Pseudonyms also help in privacy protection [4].

Authentication Methods in VANET

There are some Authentication Methods in VANETs which are discussed below [5]

Node level authentication

In Node level authentication method message is established to instigate from definite node.

Group level authentication

In Group level authentication the message is confirmed to instigate from a certain group of nodes.

Unicast authentication

In unicast authentication the message is sent to only a single node. Sometimes special messages are sent to specific node in vehicular ad hoc networks.

Multicast authentication

In multicast authentication the message is sent to various nodes. Sometimes messages are sent not to the entire nodes in the vehicular ad hoc.

Broadcast authentication

In Broadcast authentication the message is sent to each and every node in the network.

Intrusion Detection in VANET

Intrusion Detection is a first line of defense with the purpose of reducing probable intrusions but undeniably, it cannot eliminate them. Intrusion detection can help us to successfully distinguish “normal” from “abnormal” behavior. It is an essential part of reliable communication [9]. Intrusion detection system notifies the active safety system to disregard the warning and communicates the detection results to other nodes, mainly follow up nodes [10]. It is a mechanism to recognize anomalous or suspicious actions on the target analyzed. It has information of successful or failed intrusions attempts [11].

Intrusion Detection Techniques

Intrusion Detection Techniques are classified into three categories which are discussed below.

Signature based system: In this system an attack is detected if the data matched with malicious behaviors that are already registered. The system has a database behavior of confident attacks with which are evaluated the data collected. This technique may demonstrate low false positive rates, but at detecting earlier strange attacks it does not perform well [11] [12].

Anomaly detection system: In Anomaly detection system system identifies any behavior which deviates the standard pre-established behavior and set off a response or notification. This technique is able to detect formerly unknown attacks, but may show high rates of false positives [11] [12].

Specifications based system: In Specifications based system the system describes a set of circumstances that a program or protocol must satisfy. If the program or protocol does not convene the conditions set of appropriate operation then an attack is detected in network. This technique can give the ability to detect formerly unidentified attacks, whereas displaying a low false positive rate [11] [12].

Issues in Intrusion Detection and Authentication

In vehicular ad-hoc network (VANET) there are some challenges for Intrusion Detection. The main threat of Intrusion Detection is Distributed Denial-of-Services (DDoS) attacks. This attempts to make the network resource unavailable to its proposed users. Anomaly detection is not able to illustrate what the attack is and may have high false positive rate. Misuse detection systems lacks the ability to detect the truly innovative (i.e., newly invented) attacks [13]. IDS technology needs a lot of enhancements. So it is very essential for organization to clearly describe their expectations from the IDS implementation. A lot of plans are requisite in the design as well as the implementation phase of IDS. It is significant to take care of sensor to manager ratio, because a badly configured IDS sensor may send a lot of false positives to the console. The IDS technology works on attack signatures, which are attack patterns of previous attacks. The signature database wishes to be updated when an unusual attack is detected and the fix for the same is available. It is significant to keep in mind one most vital aspect of the network based IDS in switched environment while organizing a network based IDS solution [14]. There is also some issue of Authentication like Computation overhead of the system should be maintain while using authentication. The bandwidth overhead for an authentication request should be low. Authentication should be scalable and support for re-authentication and revocation procedures. Latency and Initialization time of authentication should be low.

Some papers related to authentication and intrusion detection in vehicular Ad Hoc Network have been studied under literature review section. Paper [15] and [16] discussed about intrusion detection scheme in vehicular Ad Hoc Network but these papers have some problems like in paper [15] use RADAR for location finding which is not economically efficient and scheme of paper [16] is not suitable for complex calculation. On the other hand paper [17] [19] discussed about authentication in vehicular.

In [18], the vehicles need certificate verification and revocation from the RSU, the certificates management overhead will be more. In addition to this, it handles only inside attacks only. The certificate expiration period has to be adaptively changed based on various types of attacks performed by the vehicles.

From literature review we find that for security in VANET there is a need of scheme which will be able to provide both authentication and intrusion detection. For this, we will combine authentication Intrusion detection and Authentication technique.

Literature Review

Cheng Tan *et al.* [15] have discussed about intrusion detection in vehicular ad-hoc network (VANET). The authors proposed propose a fundamental model for intrusion detection between IDS and S. The authors have analyzed the interactions between IDS and S with two-person zero-sum intrusion detection grey game for reducing the control of errors. The authors present implementation architecture of their intrusion detection scheme. The proposed model has greater flexibility than classical model. In this system RADAR is using for finding location of vehicles, but on the highways there are various type of vehicle by using radar it is very complex to distinguish their types. Use of radar is also not so efficient.

M. Mehdi *et al.* [16] have discussed about intrusion detection system in vehicular ad-hoc network (VANET). The authors have proposed a new anomaly IDS design using a parametric mixture model for behavior modeling and Bayesian based detection. This approach uses a Bayesian classification procedure associated to unverified learning algorithm to estimate the deviation between current and reference behavior and incessant re-estimation of model parameters is allow for real time operation. Recursive log likelihood and entropy estimation are used as a measure for monitoring model deprivation linked with behavior changes and the associated model update. In this approach Gaussian parametrical model is used which is not suitable for complex data, so this system is not suitable for complex data.

Lei Zhang *et al.* [17] have discussed about challenges in authentication protocols for securing vehicular ad hoc networks (VANETs). The authors proposed a new privacy-preserving authentication protocol. In this protocol, each RSU sustains an on-the-fly produced group inside its communication range. Vehicles can secretly generate V2V messages, and validate unidentified V2V messages from other vehicles and false messages can be traced by a third party. In the case of dense traffic this algorithm outperforms state-of-the-art alternatives. The performance metrics like average message delay, message loss rate and latency have been discussed in this paper. In this mechanism when arriving message exceed the processing capacity of vehicle in batch verification period, some messages are not verified and cause message loss due to the authentication mechanism.

Y. Sun *et al.* [18] have discussed about authentication scheme in vehicular ad hoc networks (VANETs). The authors proposed an efficient pseudonymous authentication scheme with strong privacy preservation (PASS) for secure vehicular communications. PASS can assure the security and privacy necessities of VANET with considerably decreased the revocation cost and the certificate updating overhead. PASS presents strong privacy preservation to the vehicles so that the opponent cannot trace any vehicle and all Roadside. The performance metrics like Revocation Overhead, Certificate Updating Overhead, Authentication Overhead and Storage Overhead has been discussed in this paper. In this approach a vehicle acquires a huge number of pseudonymous certificates and each pseudonymous certificate validates in different time slots. Hence a vehicle has to take extra certificates than it requirements.

H. C. Hsiao *et al.* [19] have discussed about basic security primitives in Vehicular Ad-Hoc Networks (VANETs). The authors proposed two flooding-resilient signature schemes which are Fast Authentication (Fast-Auth) and Selective Authentication (Sel-Auth). FastAuth protects VANET episodic single-hop beacons by leveraging the beacon inescapability and SelAuth secures multi-hop applications by punctual attack isolation. This authentication schemes can diminish signature flooding in several VANET applications. The performance metrics like overall computational overhead, average hop of invalid packets, overall communication overhead and convergence speed has been discussed in this paper. In selective authentication Digital signatures are use for neighbor authentication but it is computationally expensive.

In this proposal, we propose an Anomaly Based Intrusion Detection with Group Signature Based Authentication technique for VANET.

Proposed Solution

Overview

In this paper, we propose an Anomaly Based Intrusion Detection with Group Signature Based Authentication technique for VANET.

A trusted set of nodes (TN) are found based on the outcome of intrusion detection. Anomaly Detection scheme based on Bayesian classification is applied for intrusion detection. In this scheme first a reference behavior model for the monitored system is build. This reference behavior is modeled from observed audit data describing the use of the system by a representative set of legitimate, non-malicious entities. Then audit data related to new system activities is evaluated to detect deviations between the current and the reference behaviors. New pragmatic data is compared to the reference model by means of a Bayesian classification and cluster pertinence evaluations, if there is a difference then intrusion is detected if the both data are matched then this node is added to set of trusted node.

The trusted authority (TA) issues digital certificates for vehicles and RSUs and maintains a Certificate Revocation List (CRL) containing the certificates of revoked vehicles. The nodes which belong to TN set will get certificates with long expiration times whereas the other non-trusted nodes have very short expiration times. The RSU assigns a group signature to TN for authentication. This is a secret member key which is generated using Signcryption. A group signature permits the members of a group to sign on behalf of the group. After receiving a secret member key from an RSU, each vehicle can secretly send messages on behalf of the group maintained by this RSU.

Bayesian Classification

The aim is to model different entities profiles that could not be separated a priori by a learning procedure. Unsupervised learning is accomplished by fitting the mixture model parameters by the expectation maximization (EM) algorithm. To construct a Bayesian classification procedure based on the observations and leads to the system behavior model, a parametrical mixture model [16] is used. In unsupervised learning the model order may also be unknown, so in order to estimate a minimum entropy criterion is introduced.

The PDF of the (d-dimensional) random vector ‘x,’ for which realizations are mapped from the audit data domain, are represented by a parametrical mixture model. In such models, the realizations of x are regarded as being trials of one of the K simple models designed by a kernel probability function, with each kernel function representing the model of a user profile.

Realizations from x are not clustered, e.g. the profile of each realization yi is not observable. The mixture model fundamental expression, giving the probability of x_i, can be formally expressed as:

$$\mathrm{p}(\mathrm{x}_\mathrm{i} \mid \theta_1 ... \theta_\mathrm{k}) = \sum_{\mathrm{k}=1} \mathrm{g}_\mathrm{k}(x_i, \theta_\mathrm{k}) P(h_k) \tag{1}$$

In equation (1), X_i is the i-th observed data and $P(h_k)$ is the prior probability that a data point is generated by mixture component k and h hidden vector that indicates which source (profile) the data comes from e.g. if $H_k = 1$ if data comes from cluster k otherwise z=0

H_k are kernel distribution functions with respective parameters θ_k, each of them modeling one of the use profiles; K is the model order corresponding to the number of sources being modeled.

The mixture model represented by (1) has been increasingly used to model the distribution of a wide variety of supposed random phenomena. The unknown parameters in the model (Eq. (1)) are the set of cluster probabilities $P(h_k)$ and the parameters of kernel distribution functions of each cluster θ_k, represented by

$$\mu = [P(h_1), P(h_2), \ldots\ldots, P(h_k), | \theta_1 \ldots\theta_k)] \tag{2}$$

As the log-likelihood function evaluation at the point represented by the parameter fitted by the EM-algorithm is not guaranteed to be a global maximum, a finite number of random initializations of the parameters are realized and the EM-algorithm is executed at different times.

The EM algorithm permits both log-likelihood and model parameter estimation to be done in an iterative manner.

In the particular case of Gaussian mixture models (GMM), e.g. mixture model with Gaussian kernel functions, which is used in our experiments presented further, the Eq. (1) should be rewritten replacing the general distributions (h_k) by the normal distribution (represented by φ) and the distribution parameters θk by the mean vector (μ_k) and covariance matrix (R_k), as stated at Eq. (3), where the probability $p(h_k)$ are also replaced by the weighting factor w_k, for notation simplicity.

$$P(x_i) = \sum_{k=1}^{k} w_k \phi(yx, \mu_k, R_k) \tag{3}$$

For completeness, we provide the EM recursion equations for the Gaussian mixture models:

$$P(k|x_i) = \frac{w'_k \phi(x_i, \mu_k^i, R_k^i)}{\sum_{k=1}^{k} w^i{}_k, \phi(x_i, \mu_k^i, R_k^i)} \tag{4}$$

For the purpose of the EM-algorithm, the model order K (which corresponds to the number of partitions or data sources, when using parametric mixture models for partitioning data) must be provided. Since the number of partitions is not known a priori, it is useful to be able to estimate the most probable number of partitions, as well.

Our objective is to build an “ideal partitioning” estimation for K, which should be regarded as having the posterior probability $P(k|x_i)$ (Eq. (4) in the GMM case) close to unity for one value of k and close to zero for all the others, for each realization.

The ideal partitioning should be obtained by minimizing Shannon entropy given observed data, which can be evaluated for each observation by Eq. (4):

s_K is the expected value of this entropy is evaluated taking the mean all observed data and it is calculated using the following equation

$$E^{*}(s_K) = \frac{\sum_{i=1}^{n}\sum_{k=1}^{k} P(k|\, x_i)\log(P(k|\, x_i))}{n} \tag{5}$$

In equation (5), E* denotes an expectation estimator and S_k is the measure in question.

We proceed by fitting K_{max} models with different order (K = 1, 2,...Kmax) and we evaluate the expected entropy for each case. The resulting model in a minimum of this measure will be considered the optimum model.

The complete algorithm of the learning phase, used to obtain a mixture model fitted with the EM-algorithm and with optimal model order (K) estimation can be summarized as follows:

```
Start
Define K = variable value (initially ‘0’)
        $K_{opt} = 1$
        $S_{opt} = 0$
 Using the EM-Algorithm fit the K-order model using the equation eq. (2,3)
Calculate the expected value of $S_k$ using eq. (4)
If ($S_k < S_{opt}$)
{
        $S_{opt} = S_k$ ;
        $K_{opt} = k$;
        $\mu = \mu_{opt}$;
 }
If ($K<K_{opt}$)
        K =k+1;
 Update actual model order K with optimal order ($k = k_{opt}$)
Update the actual model parameters μ with optimal model parameters $\mu_{opt}$
End
```

Algorithm 1: EM-algorithm

Anomaly Detection

The behavior model has been already fitted and is available for finding inferences in a new data presented to the system during detection. The aim is to define some penalty λ, which varies from 0 to 1 (e.g. $0 \leq \lambda \leq 1$), indicating the degree of normality concerning this realization from certainly abnormal ($\lambda = 0$) to a certainly normal ($\lambda = 1$) behavior.

Many different approaches for defining such criteria from the behavior statistical model represented by Eq. (1) are possible. We have defined a detection procedure formed by two basic steps: a (Bayesian) classification inference and a cluster pertinence inference [4]. The classification inference is straightforward for parametrical mixture models and consists of evaluation of the posterior cluster probabilities conditioned to new data x’,

$$P(k \mid x'), \quad \text{for}\,(k = 1,2.....k) \tag{6}$$

The complex one is Cluster pertinence inference. As all the kernel distributions used in our model have a continuous nature, considering data posterior probabilities conditioned to cluster probability, p(x'| k), by simple evaluation of the cluster probability density function is meaningless.

A more realistic approach consists in evaluating the probability of new data being contained in some pertinence interval (P_k), defined as a function of cluster distribution parameters (µk and Rk, for instance) and the observation x', which should be formally expressed as

$$P(x' \in P_k \mid)k) = \int h_k(x, \theta_k) d\, P_k \tag{7}$$

In equation (7), P_k is probability and it look like some kind of cumulative distribution function, if we define P_k is as follows

$$P_k = \mid x \in R^d \mid \frac{\| x - \mu_k \|^2}{\| R_k \|} \geq \gamma^2 \mid \tag{8}$$

In equation (8), $\| \|^2$ and | | are norm operators and γ is a constant that is dependent on x'. Finally, detection penalty should be defined as

$$\lambda(x') = \sum p(k \mid x')\, P(x' \in P_k \mid k) \tag{10}$$

A trusted set of nodes (TN) are found based on the outcome of intrusion detection. Anomaly Detection scheme based on Bayesian classification is applied for intrusion detection. New pragmatic data is compared to the reference model by means of a Bayesian classification and cluster pertinence evaluations, if there is a difference then intrusion is detected if the both data are matched then this node is added to set of trusted nodes {TN.}

Signcryption

The trusted authority (TA) issues digital certificates for vehicles and RSUs and maintains a Certificate Revocation List (CRL) containing the certificates of revoked vehicles.

Trust Authority (TA)

Issuing the digital certificates for vehicles and RSUs is the responsibility of TA. It maintains a Certificate Revocation List (CRL) containing the certificates of revoked vehicles. It is a trusted authority and can be viewed as an electronic counterpart of the traffic administration office in the real world. The TA owns the system's master key which is used to issue digital certificates for vehicles and RSUs. It also maintains a Certificate Revocation List. The TA is assumed to be completely trustable, hard to compromise, and powerful, i.e. with sufficient computation and storage capacity.

Traffic Manager (TM)

It is the tracing manager. It can be instantiated by the traffic police. It is able to trace the identity of a vehicle having generated a certain safety message.

Road Side Unit (RSU)

RSUs are densely distributed in the roadside and RSUs are used to issue secret member keys to vehicles and assist the TM to efficiently track the real identity of a vehicle from any safety message.

The nodes which belong to TN set will get certificates with long expiration times whereas the other non-trusted nodes have very short expiration times. The RSU assigns a group signature to TN for authentication. This is a secret member key which is generated using Signcryption [17]. A group signature permits the members of a group to sign on behalf of the group. After receiving a secret member key from an RSU, each vehicle can secretly send messages on behalf of the group maintained by this RSU.

The signcryption scheme is used to help a vehicle to receive a secret member key from an RSU secretly. It is a public-key primitive which has the ingredients of both digital signature and data encryption.

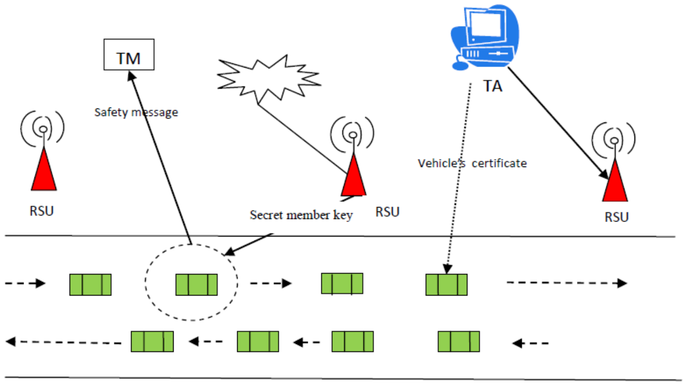

Figure 1: Network Model

The signcryption is used to help a vehicle to obtain a secret member key from an RSU secretly, and the group signature scheme is used for V2V communications.

Table 1: Notation Used In This Paper

R_i	*i*-th RSU
RSU	Responsible for issuing secret member keys for vehicles
V_i	The i-th vehicle
V_{id}	Vehicle identity
TS	Time Stamp
certR_i	Certificate of R_i
certV_i	Certificate of V_i

SM	Safety Message
SK	Session Key
Ex()	Encryption
Dx()	Decryption
PB	Public key
PK	Private key

For each vehicle, RSU issue secret member keys. In this stage a vehicle joins a group maintained by an RSU. An RSU is assumed to be more powerful than a vehicle, and its communication is range longer. RSUs are distributed in the roadside and they broadcast their certificates and the ones of their adjacent RSUs.

When V_i passes by R_i, if V_i is already a member of the current group maintained by R_i, then R_i does nothing. Otherwise, V_i requests a secret member key from R_i by using the KeyRequest protocol:

KeyRequest: This is an interactive protocol and it run between V_i and R_i. V_i has private/public keys pk V_i/pbV_i and certificate CertV_i. Ri has private/public keys pk R_i/pbR_i and certificate CertR_i . This protocol employs the signcryption scheme described in [17] and consists of three steps:

1) At this step, Vi takes as input SK, TS, CertV_i , V_i to generate a signcrypted message and sends the signcrypted message to R_i. To do this, V_i does the following:
   a) Each vehicle chooses a session key SK.
   b) Select a random r ∈ Z∗ q, and compute
      $\sigma = \mathrm{H1}(\mathrm{SK} \,\|\, \mathrm{CertV_i} \,\|\, \mathrm{TS} \,\|\, \mathrm{s} \,\|\, \mathrm{pbR_i} \,\|\, \psi(\mathrm{pbR_i^r}))$
      $\lambda = (\mathrm{SK} \,\|\, \mathrm{TS} \,\|\, \mathrm{CertV_i} \,\|\, \sigma) \oplus H2(\mathrm{s} \,\|\, \mathrm{pbR_i} \,\|\, \psi(\mathrm{pbR_i^r}))$
   c) Send $\rho = (s, \lambda)$ to R_i
2) After receiving $\rho = (s, \lambda)$ from V_i, R_i first designcrypts ρ to get the plaintext. It checks the validity of the signature and the certificate in the plaintext. If they are valid, a secure channel between R_i and V_i is opened. Through this secure channel, a secret member key will be returned to V_i. The concrete procedure is as follows
   a) Compute the plain text $(\mathrm{SK} \,\|\, \mathrm{TS} \,\|\, \mathrm{CertV_i} \,\|\, \sigma) = \lambda \oplus H2(s \,\|\, pbR_i^r)$
   b) Check the validity of CertV_i. if it is invalid abort it, otherwise extract pkV_i from CertV_i
   c) Verify the signature by checking $e(\sigma) = \mathrm{e}(\mathrm{H1}(\mathrm{SK} \,\|\, \mathrm{CertV_i} \,\|\, \mathrm{TS} \,\|\, \mathrm{s} \,\|\, \mathrm{pbR_i} \,\|\, \mathrm{pbR_i^r}), \mathrm{pkV}_i)$
      If the check is satisfied, using pbV_i, generate a tuple (ηi, θi): select θi ∈ Z∗
   d) Compute k = E_{SK}((TS||ηi||θi)) and send k to V_i.
   e) Store (CertV_i , η_i) to R_i's database
3) When V_i receives k from R_i, it computes (TS' ||ηi||θi) = D_{SK}(k). If TS = TS′, V_i accepts the secret member key (ηi, θi), where TS is the timestamp used by V_i in the first step. The Certificate Revocation List (CRL) contains the RSU list.

A signcryption scheme allows a sender to simultaneously sign and encrypt a message. An attractive point is that it takes less computational time and has lower message expansion rate than the sign-then-encrypt procedure.

Simulation Results

Simulation Model and Parameters

The Network Simulator (NS2) [20], is used to simulate the proposed architecture. In the simulation, 82 mobile nodes move in a 2500 meter x 700 meter region for 50 seconds of simulation time. All nodes have the same transmission range of 250 meters. The simulated traffic is Constant Bit Rate (CBR).

The simulation settings and parameters are summarized in table.

No. of Nodes	82
Area Size	2500 X 700
Mac	IEEE 802.11
Transmission Range	250m
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	512
Rate	50kb
Attackers	1,2,3,4,5 and 6

Performance Metrics

The proposed An Anomaly Intrusion Detection with Group Signature Based Authentication (ADGSA) is compared with the Pseudonymous Authentication Scheme with Strong privacy preservation (PASS) technique [18]. The performance is evaluated mainly, according to the following metrics.

- **Packet Delivery Ratio:** It is the ratio between the number of packets received and the number of packets sent.
- **Packet Drop**: It refers the average number of packets dropped during the transmission
- **Delay**: It is the amount of time taken by the nodes to transmit the data packets.
- **Throughput**: It is the total number of data packets received by the receiver.

Results

1) Based on Attackers

In our first experiment we vary the number of attackers as 1, 2,3,4,5 and 6.

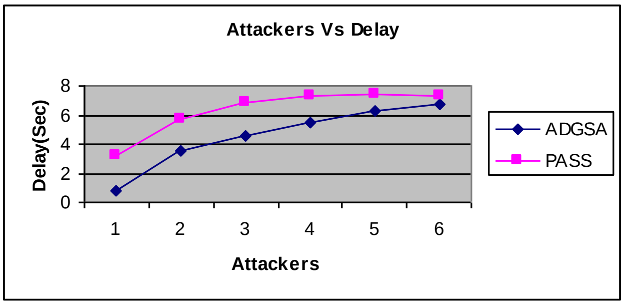

Figure 2: Attackers Vs Delay

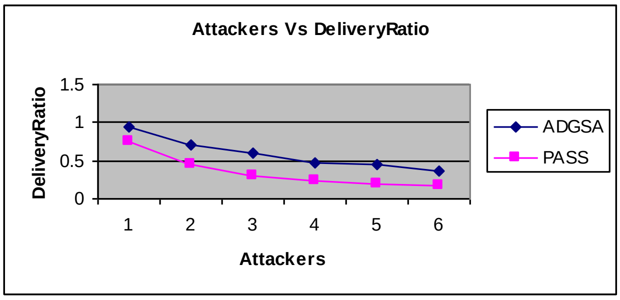

Figure 3: Attackers Vs Delivery Ratio

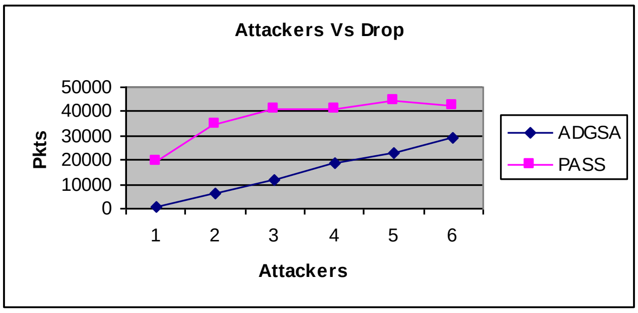

Figure 4: Attackers Vs Drop

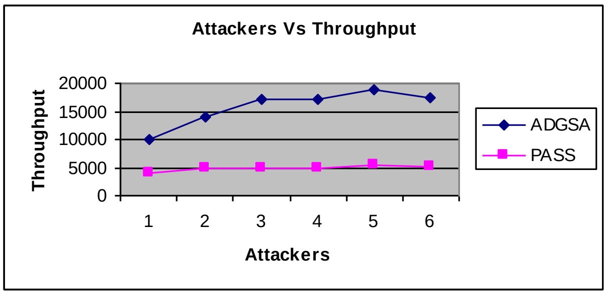

Figure 5: Attackers Vs Throughput

Figure 2 shows the delay of ADGSA and PASS techniques for different number of attacker scenario. We can conclude that the delay of our proposed ADGSA approach has 32% of less than PASS approach.

Figure 3 shows the delivery ratio of ADGSA and PASS techniques for different number of attacker scenario. We can conclude that the delivery ratio of our proposed ADGSA approach has 45% of higher than PASS approach.

Figure 4 shows the drop of ADGSA and PASS techniques for different number of attacker scenario. We can conclude that the drop of our proposed ADGSA approach has 64% of less than PASS approach.

Figure 5 shows the throughput of ADGSA and PASS techniques for different number of attacker scenario. We can conclude that the throughput of our proposed ADGSA approach has 68% of higher than PASS approach.

Conclusion

We proposed an Anomaly Based Intrusion Detection with Group Signature Based Authentication technique for VANET. A trusted set of nodes (TN) are found based on the outcome of intrusion detection. Anomaly Detection scheme based on Bayesian classification is applied for intrusion detection. Then audit data related to new system activities is evaluated to detect deviations between the current and the reference behaviors. The trusted authority (TA) issues digital certificates for vehicles and RSUs and maintains a Certificate Revocation List (CRL) containing the certificates of revoked vehicles. The nodes which belong to TN set will get certificates with long expiration times whereas the other non-trusted nodes have very short expiration times. The RSU assigns a group signature to TN for authentication. This is a secret member key which is generated using Signcryption. A group signature permits the members of a group to sign on behalf of the group. After receiving a secret member key from an RSU, each vehicle can secretly send messages on behalf of the group maintained by this RSU.

References

[1] Ayonija Pathre, Chetan Agrawal and Anurag Jain, "*Identification of Malicious Vehicle in Vanet Environment from Ddos Attack*", Journal of Global Research in Computer Science, Volume 4 No 6, 30-34, ISSN-2229-371X, June 2013

[2] Brijesh Kumar Chaurasia and Shekhar Verma, "*Infrastructure based Authentication in VANETs"*, International Journal of Multimedia and Ubiquitous Engineering, Vol. 6, No. 2, April, 2011

[3] M.Erritali, B. EL Ouahidi, B.Hssina, B. Bouikhalene and A. Merbouha, "*An Ontology-Based Intrusion Detection for Vehicular Ad Hoc Networks"*, Journal of Theoretical and Applied Information Technology, Vol. 53 No.3, and ISSN: 1992-8645, 31st July 2013.

[4] Sushmita Ruj, Marcos Antonio Cavenaghi, Zhen Huang, Amiya Nayak, and Ivan Stojmenovic, "*Data-centric Misbehavior Detection in VANETs*", Vehicular Technology Conference (VTC Fall),5-8 Sept, 2011, IEEE, ISSN: 1090-3038, Print ISBN: 978-1-4244-8328-0. doi>10.1109/ VETECF.2011.6093096

[5] Khalid Haseeb, Dr.Muhammad Arshad, Dr.Shazia Yasin and Naveed Abbas, "*A Survey of VANET's Authentication*", Liverpool John Moores University, ISBN: 978-1-902560-24-3 © 2010 PGNet, Jun 2010

[6] Huang Lu, Jie Li and Mohsen Guizani, "*A Novel ID-based Authentication Framework with Adaptive Privacy Preservation for VANETs",* Computing, Communications and Applications Conference (ComComAp) IEEE, 11-13 Jan. 2012, Print ISBN: 978-1-4577-1717-8, doi: 10.1109/ComComAp.2012.6154869

[7] Irshad Ahmed Sumra,Iftikhar Ahmad, Halabi Hasbullah and Jamalul-lail bin Ab Manan, "*Classes of Attacks in VANET*", Electronics, Communications and Photonics Conference (SIECPC),Saudi International, IEEE, 24-26 April 2011, Print ISBN: 978-1-4577-0068-2, doi: 10.1109/SIECPC.2011.5876939

[8] Mrs.Kadam Megha V, "*Security Analysis in VANETs: A Survey",* International Journal of Engineering Research & Technology (IJERT) Vol. 1 Issue 8, October - 2012, ISSN: 2278-0181.

[9] Aikaterini Mitrokotsa, Manolis Tsagkaris and Christos Douligeris, *"Intrusion Detection in Mobile Ad Hoc Networks Using Classification Algorithms*", IFIP International Federation for Information Processing Volume 265, 2008, pp 133-144

[10] Tim Leinm¨uller, Albert Held, G¨unter Sch¨afer and Adam Wolisz, *"Intrusion Detection in VANETs",* 12th IEEE International Conference on Network Protocols (ICNP 2004), Student Poster Session, Berlin, Germany, October 5th - 8th, 2004

[11] Mohammed ERRITALI, Bouabid El Ouahidi, *"A Survey on VANET Intrusion Detection Systems",* International Journal of Engineering and Technology (IJET) ISSN: 0975-4024 Vol 5 No 2 Apr-May 2013

[12] Paul Brutch and Calvin Ko, *"Challenges in Intrusion Detection for Wireless Ad-hoc Networks",* SAINT-W '03 Proceedings of the 2003 Symposium on Applications and the Internet Workshops (SAINT'03 Workshops), Page 368 , IEEE Computer Society Washington, DC, USA ©2003, ISBN:0-7695-1873-7

[13] Yongguang Zhang, Wenke Lee and Yi-An Huang, *"Intrusion Detection Techniques for Mobile Wireless Networks",* Wireless Networks, Volume 9 Issue 5, September 2003, Pages 545 - 556, ISSN: 1022-0038, doi>10.1023/A:1024600519144

[14] SANS Institute InfoSec Reading Room, "*A Paper On Intrusion Detection System*", © SANS Institute 2001, As part of the Information Security Reading Room.

[15] Cheng Tan, Hao Sun, Ning Cao, Lihui Sun, Cheng Li, "*A Novel Grey Game-Theoretic Model for Intrusion Detection in Vehicular Ad Hoc Network*", ICCSEE-13, Advances in Intelligent Systems Research, ISBN:978-90-78677-61-1, ISSN: 1951-6851, doi:10.2991/iccsee.2013.140, January 2013

[16] M. Mehdi, S. Zair, A. Anou and M. Bensebti, *"A Bayesian Networks in Intrusion Detection Systems"*, Journal of Computer Science 3 (5): 259-265, 2007, ISSN 1549-3636 © 2007 Science Publications

[17] Lei Zhang, Qianhong Wu, Agusti Solanas and Josep Domingo-Ferrer, "*A Scalable Robust Authentication Protocol for Secure Vehicular Communications"*, Vehicular Technology, IEEE Transactions Volume: 59, Issue: 4, May 2010, ISSN: 0018-9545, INSPEC Accession Number: 11285973, doi: 10.1109/TVT.2009.2038222

[18] Yipin Sun, Rongxing Lu, Xiaodong Lin, Xuemin (Sherman) Shen and Jinshu Su, "*An Efficient Pseudonymous Authentication Scheme with Strong Privacy Preservation for Vehicular Communications",* Vehicular Technology, IEEE Transactions, Volume:59 , Issue: 7 , Sept. 2010, Pg3589 - 3603, ISSN : 0018-9545, INSPEC Accession Number: 11523632, doi : 10.1109/TVT.2010.2051468

[19] Hsu-Chun Hsiao, Ahren Studer, Fan Bai, Bhargav Bellur and Aravind Iyer, *"Flooding-Resilient Broadcast Authentication for VANETs"*, MobiCom '11, 17th annual international conference on Mobile computing and networking, Pages 193-204, ISBN: 978-1-4503-0492-4, doi>10.1145/2030613.2030635, 2011.

[20] Network Simulator: http:///www.isi.edu/nsnam/ns