ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

A NOVEL THRESHOLD BASED ANONYMOUS AUTHENTICATION PROTOCOL FOR VANET

V. Mathimalar M.Sc., M.Phil., M.B.A.,
Assistant Professor, Department of Computer Science, MCA and IT & Applications,
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India.

B. Yogapriya
Research Scholar, Department of Computer Science
Shrimati Indira Gandhi College, Trichy, Tamilnadu, India

Abstract

Since Vehicular ad hoc networks (VANETs) are vulnerable to various kinds of attacks, there is a need tofulfill the security requirements like message privacy,integrity, and authentication. The authentication techniqueis said to be efficient if it detects compromised nodesaccurately with less complexity, reduced authenticationdelay, and keying overhead. In this paper, a threshold-basedauthentication scheme for cluster-based VANETs is proposed.The vehicles are clustered, and the threshold degree of each node is estimated. The threshold degree is a combinationof direct threshold degree and indirect threshold degree. Based onthis estimated threshold degree, cluster heads are selected.Then, each vehicle is monitored by a set of verifiers, andthe messages are digitally signed by the sender andencrypted using a public/ private key as distributed by athreshold authority and decrypted by the destination. Thisverifies the identity of sender as well as receiver thusproviding authentication to the scheme. By simulationresults, we prove that the proposed technique provides highsecurity with less overhead and delay.

Keywords: Vehicular Ad Hoc Network, Clustering, Threshold Authentication, Threshold Authority, Monitoring.

1. Introduction

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

VANET is made up of extremely mobile automobiles with sparingly installed stations at the sides of the road; all ofthem provided with gadgets as well as sensing devices insome cases, that communicate wirelessly. By making useof vehicle-to-vehicle (V2V) ad hoc mode as well asbetween vehicles and roadside stations by means of vehicle-to-road (V2R) or vehicle-to infrastructure (V2I) communicationmode through a base station (BS) or accesspoint (AP), wireless communication can be achieved. Forthis communication to take place, the AP is usuallydeployed down the road contained by the BS or AP rangefor transmission [1]. On board units (OBUs) are deployedon these automobiles in order to enable them and the unitsalong the road, comprising the infrastructure connectingthe vehicular network to the central unit. VANET facilitatesdata transmission such as messages indicating cautionrelated to road situation, traffic condition, and drivingcondition of the drivers. Application of VANET includeaccumulating, processing, allocating and delivering theinformation about the road in real time [2–5].

The increased movement of the vehicles as a result of the repeatedly altering topology imposes a crucial task indelivering unicast communication among vehicles itself orbetween vehicles and the concerned infrastructure [4, 6].

With the increase in distance, the energy required to provide good quality communication also increases. As aresult, the overall energy consumed by the transceiver willbe high. On the basis of the number of the relaying nodesand transmission distance between every pair of nodes, theenergy consumed increases during communication inmulti-hop VANET. Therefore, the energy required for asingle transmission amplifies nonlinearly, in the case oflittle hops and higher transmission distances. So, to obtainthe best energy efficiency, we need to maintain a tradeoff between the hop number and the transmission range forevery hop [3, 7].

The target of VANET is achieving higher level of safety on the road. In order to achieve it, every vehicle working asa sensor sends information to each other like warningsrelated to the present speed, physical location and ESPactivity, which lets the

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

drivers to take appropriate measuresin case of hazardous condition like accidents, trafficproblem, and glaze. Also, official vehicles used by thepolice and the firefighters can make use of it to transfermessages for stopping other vehicles or clearing the road.Moreover, services on the basis of location and Internetalong the road can be provided by VANET. Withregard to the protection concerns, reliability, privacy, andaccessibility that are the safety and confidentialityrequirement, it is required for the three application divisionslike warnings and telematics information, alarmsignals and instructions, and value-added services. There isa need of a secure topology maintaining threshold and allowingcryptography process [8, 9]. Jamming, impersonation,privacy violation, forgery, in-transit traffic tampering, onboardtampering, and so forth are the situations to whichVANETs are vulnerable. Therefore, there is a need forVANET to fulfill the security requirements like messageprivacy and integrity, message non negation, unit validation,admission management, secrecy, accessibility, andresponsibility identification [10, 11].

2. Problem Identification

Achieving energy proficiency as well as security is a challenge in VANET. With the help of cryptographictheory [4], signature using cryptography [12], privacypreservation [13], threshold models [14, 15], anonymous credential[16], and collaborative protocol [17], the works[4, 12–17] have guaranteed secure networks. But, certainissues still exist in the current network such as powerconsumption [3], incapacity to discover compromisednodes [4], complexity [12], message dropping [13], higherdelay [14], overhead [15], and collision [17].

Hence, an objective is to develop a scheme in VANET with ability to detect compromised nodes, less complexity,reduced message dropping, delay, overhead, and collision.

By using the clustering technique and the key distribution mechanism, security can be accomplished in VANET,where the vehicles are gathered together in clusters and

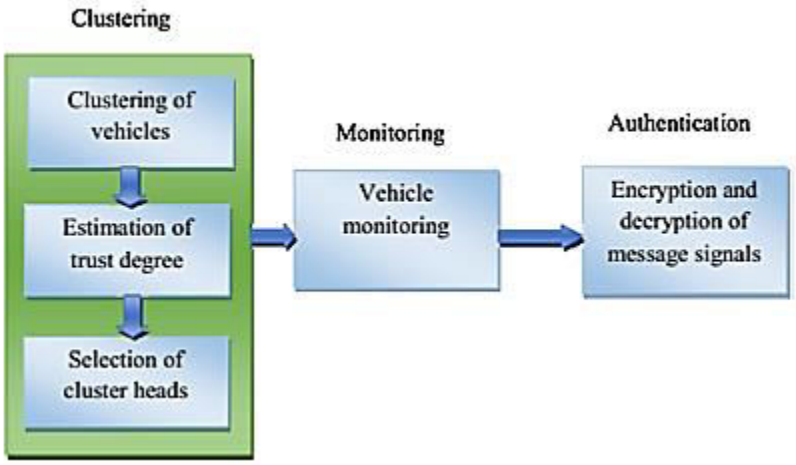
ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

theproblematic vehicles are secluded by a particular algorithm[12]. Later, on the basis of the proxy signature which isencrypted and transmitted through a safe channel, keys areproduced. But, this mechanism is very complicated, andthere are possibilities for the VANET to break down, onhigh rate of network utilization leading to reduced energy. The privacy and integrity requirement has not yet been fulfilled in VANET.

3. Threshold based Authentication Technique

Aim of this paper is to develop a threshold based authentication scheme for cluster based VANETs. In thisscheme the vehicles are clustered [12] and the thresholddegree of each node is estimated. The threshold degree is acombination of direct threshold degree and indirect thresholddegree. Direct threshold degree of node is calculated fromneighbors using past interactions whereas indirect thresholddegree is recommendation threshold degree from the mostsimilar nearest neighbors. Based on this estimated thresholddegree, the cluster heads (CH) are selected. Then eachvehicle is monitored by a set of verifiers. Then we adddigital signature to the messages signed by the sender andencrypted using a public/ private key as distributed by athreshold authority and decrypted by the destination. Thisverifies the identity of sender as well as receiver thusproviding authentication to the scheme.



ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Figure 1: Block Diagram for Threshold based Authentication scheme

3.1 Adversarial Model

The attacks in VANET are of two types. They are active attack and passive attack. In a passive attack, the attackereavesdrops but does not modify the message, whereas in anactive attack, the attacker may transmit messages, replayold messages, modify messages in transit, or delete selectedmessages. Man-in-the-middle and replay attacks areconsidered in the proposed work. Man-in-the-middle attackis an active attack in which the attacker secretly relays andalters the communication between two parties who believethat they are directly communicating with each other.Replay attack is also an active attack in which the attackermay repeat the data or delay the data. Node-to-nodeauthentication (described below) is used to address theseattacks (Fig. 2).

3.2 Clustering of Vehicle

We assume that there are several Certification Authorities (CAs) in the network, where each CA can authenticate allthe vehicles located inside its region. A CA is a thresholdthird party that manages identities, cryptography keys, andcredentials of vehicles.

Initially the vehicles are divided into several clusters in a highway environment with two bands and each bandhaving three lanes. Each cluster consists of one clusterhead (CH) and one or more members. Vehicles in onecluster are linked directly and vehicles that are located intwo different clusters can communicate together via theirCHs. Each vehicle can play the role of a CH or gateway ormember. If one vehicle is located within two or moreclusters, it is called a gateway. Each CH maintains theinformation about its members and gateways.The cluster head election process is described in Algorithm 1.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

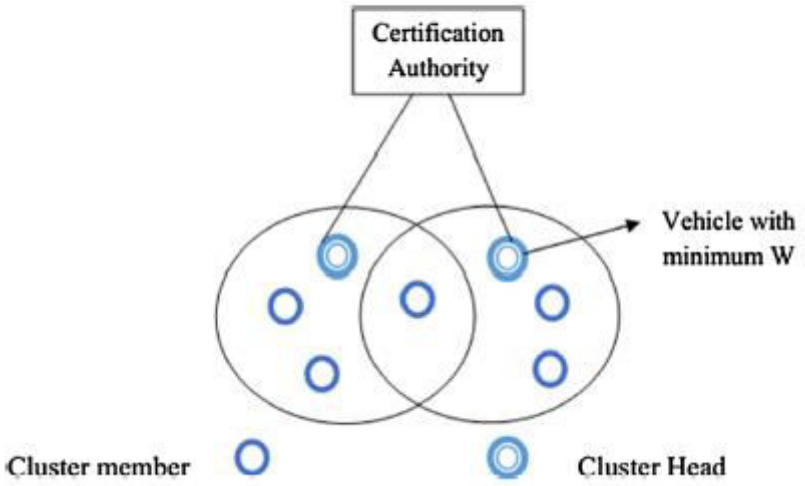


Figure 2: Cluster Formation and Cluster Head Selection

Table 1: Algorithm notation and its description

Notation	Description
V_i	Each Vehicle in the network, i=1,2,3…….
V_j	Neighbor of V_i
Add_i	Address of V_i
Id	Id of V_i
Nl_j	Neighbor list ofV_j
D_{ij}	Distance between$V_j$and V_i
NV_j	Number of neighbors ofV_j
R	Dynamic transmission range
θ	Direction of vehicle
S	Speed of the vehicle
DTr	Threshold degree
$\alpha, \beta, \delta, \gamma, \eta$	Weighting Constants

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Step 1: Each vehicle V_i declares itself as a CH and broadcast the bacon $B[add_i, Id_i]$

Step 2: Each vehicle$V_j$createsNl_jafter receiving$B[add_i, Id_i]$ from each V_i.

Step 3: Then$V_j$estimatesD_{ij}.

Step 4:V_j calculates a weighted sum

$$W_j = \alpha.NV_j + \beta.R + \delta.\theta + \gamma.S - \eta.DTr \qquad (1)$$

Step 5: The parameters used in the Eq. (1) are calculated by the vehicle. The weighted constants range from 0 to 1.As the weighted sum is calculated based on theseparameters, the CH which is selected based on it willbe threshold and efficient.

Step 5: Then $V_k$withW_k = Minimum is selected as CH.

3.3 Estimation of Threshold Degree

Threshold degree estimation is done for the selection of Cluster Heads (CH). Threshold relationships made from the directinteractions is described as direct threshold. The threshold relationshipbuilt from the trust node or the chain of trust nodeis called as indirect threshold node [14].The direct threshold degree from vehicle p to vehicle q is given by,

$$T_{new}^{old}(p,q) = \begin{cases} T_{new}^{old}(p,q) + RF, (ST > 0) \\ T_{new}^{old}(p,q) - RF, (ST > 0) \end{cases} \qquad (2)$$

where

T_{old} = Previous threshold degree (i.e., the value calculated during previous CH selection process).

RF—Reward factor,

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

PF—Penalty factor,

ST, FT—Number of successful and failed transactionsbetween Told and T_{new}in time interval Δt.

The indirect threshold degree from vehicle p to vehicle q is given by,

$$T^{r}_{(p,q)} = \frac{\sum_{k \in m} T^{d}(k,q) * s(p,k)}{\sum_{k \in m} s(p,k)}$$

K—common neighbor vehicle

s(p,k)—similarity of values of vehicle p and k.

m—number of most similar nearest-neighbors of p andq.

The estimation of threshold degree is the sum of direct thresholdand indirect threshold,

$$T(p,q) = \alpha \times T^{d}(p,q) + \beta \times T^{r}(p,q)$$

α $and \beta$ – weighting factors for $T^{d}(p,q)$ and $T^{r}(p,q)$

Table 2: Notation and Description of the algorithm2

Notation	Description
T(p,q)	Threshold degree between vehicle p and q
N(p)	Neighbor of node p
T^{d}	Direct threshold degree
T^{r}	Indirect threshold degree
tc	Current time

Step 1: Node p collects the local topology information.

Step 2: T^{d} is calculated by p based on the neighbor table and historicalevents with N(p) using (2).

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

Step 3: If there is no interaction between the p and q, then\

Step 4: $T(p,q) = T^d$

Step 5: Store T^d and tc in local information table

Step 6: End if

Step 7: If there is interaction between p and q, then

Step 8: UpdateT^d

Step 9: $T^r$is calculated by p by estimating similarT^dvalues of N(p) to q, using (3)

Step 10: Calculate T(p, q) using (4)

Step 11: End if

3.4 Vehicle Monitoring

In monitoring phase, a set of verifier nodes collect information about the behavior of all vehicles in a cluster. Avehicle V_i can be a verifier of another vehicle V_j if$T(V_i)>T(V_j)$, where T is the total threshold degree stored inthe neighbor table of each node. Let T_{min} be the minimumthreshold value of threshold degree. The steps involved in thevehicle monitoring process are illustrated in Algorithm 3.

Table 3: Notation and its description of algorithm3

Notation	Description
T_{min}	Minimum threshold value of threshold degree
$T(V_j)$	Total threshold degree of vehicle V_j
CA	Certificate authority
RSU	Road side unit

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

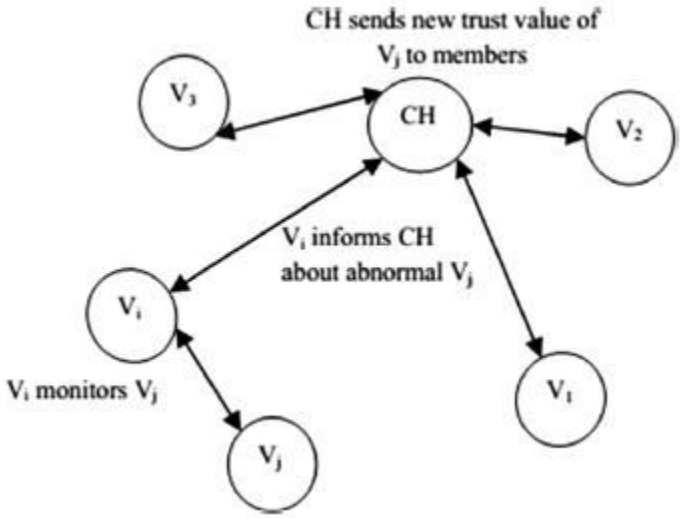


Figure 3: Vehicle Monitoring

Step 1: $\{V_j\}$ detect the abnormal behaviors of vehicle $V_j$by monitoring, whenV_j acts as a relay node or source node.

Step 2: After detecting abnormal behavior of V_j, the CH requests for the threshold degree of V_j from other verifiers in the cluster.

Step 3: When $T(V_j)$ is different from its old value, the new value of $T(V_j)$ is informed by the CH to the other cluster members.

Step 4: All other cluster members updates their neighbor table based on the new value of $T(V_j)$.

Step 5: new $T(V_j)>= T_{min}$, thenAll other cluster members cooperate with V_j.

Step 6: Else

Step 7: CH informs the id of V_j to the CA.

Step 8: CA broadcasts the ID of V_j to all the vehicles and RSUs.

Step 9: End if

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

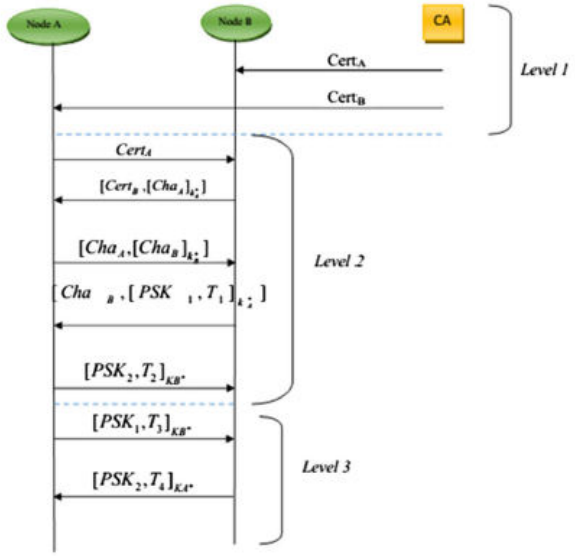
3.5 Node to Node Authentication

Initially, we assume that public/private key pairs and certificates are distributed to legitimate nodes who wish to jointhe ad hoc network. The keys can be entered manually orthrough secure transfer protocols. The messages sent by avehicle can be protected using digital signature (DS). Thesender attaches a DS at the end of every control message. The DS consists of a value that is known by the signer andthe content of the message being signed. The sender signsthe message using the private key and the receiver verifiersthe message with the signer's public key [15].

During the authentication procedure, the node attempting to authenticate presents its identity and certificate to theauthenticating node. The authenticating node will firstverify the certificate using the public key of CA and thenchallenge the initiating node by encrypting a nonce withthe initiating node's public key, to test whether it has thecorresponding private key. At the end of the handshake,two nodes exchange secret keys (encrypted with other'spublic key) for quick re-association in the future.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018



Notations and expressions:	
$K_i^- - i$'s private key	$Cert_i = [K_i^+, ID_i]_{K_{ac}^-}$
$K_i^+ - i$'s public key	$[X]_{K_i^-} - i$'s digital signature of content X
$Cha_i -$ Challenge	$[X]_{K_i^+}$ – Content X encypted with i's public key
$PSK_i -$ Session share key	$T_i -$ Timestamp

Figure 4: Node to node authentication

3.6 Steps involved in threshold based authentication

The entire steps involved in the threshold based authentication technique can be summarized as:

(a) Initially the vehicles are clustered.

(b) Threshold degree of each node is estimated based ondirect and indirect threshold degrees.

(c) In each cluster, cluster head is selected based on theweighted sum.

(d) Vehicles are monitored by a set of verifiers in eachcluster.

(e) The threshold degrees of vehicles with abnormal behaviorare checked by CH.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

(f) Abnormal nodes with least threshold degree are isolatedby the CA.

(g) In node to node authentication, a digital signature isadded to the messages signed by the sender andencrypted using a public/ private key as distributedby a trust authority and decrypted by thedestination.

(h) The sender signs the message using the private keyand the receiver verifiers the message with thesigner's public key.

(i) At the end of the handshake, two nodes exchangesecret keys for quick re-association in the future.

4. Simulation Result and Discussion

The proposed Threshold based Authentication Technique (TBAT) is compared with Secure scheme based on Clustering and Key Distribution (SCKD) [12] and VSPN [16]. The performance is evaluated in terms of Packet delivery ration, authentication delay, key overhead and detection accuracy.

Table 4: Parameter Setting for simulation

Number of nodes	72
Area size	2500 9 700 m
Number of BANDS	2
Number of lanes per band	3
Radio range	250, 300, 350 and 400 m.
Simulation time	50s
Packet size	512 bytes
Antenna	Omni Antenna

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

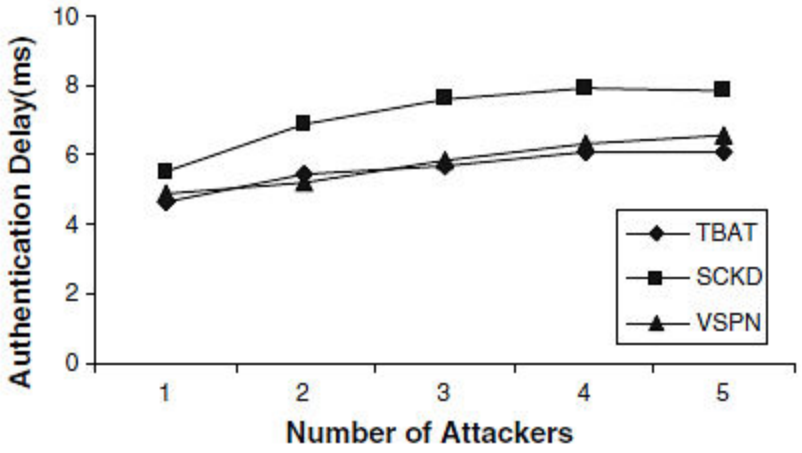


Figure 5: Attackers versus authentication delay

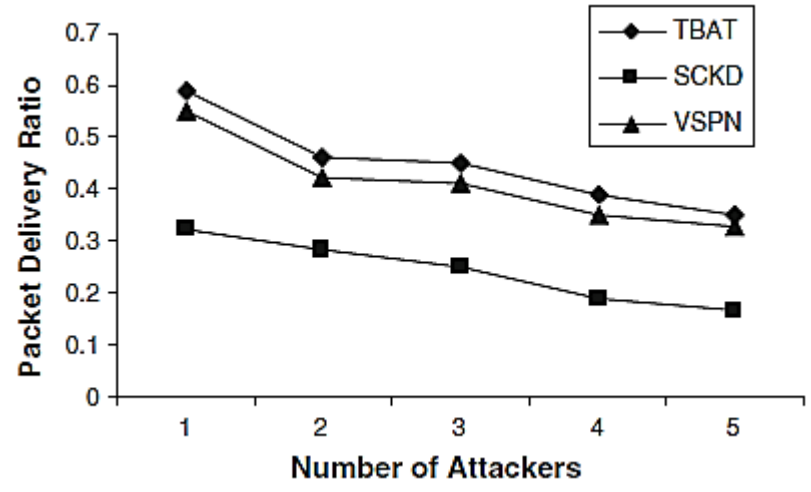


Figure 6: Attackers versus delivery ratio

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

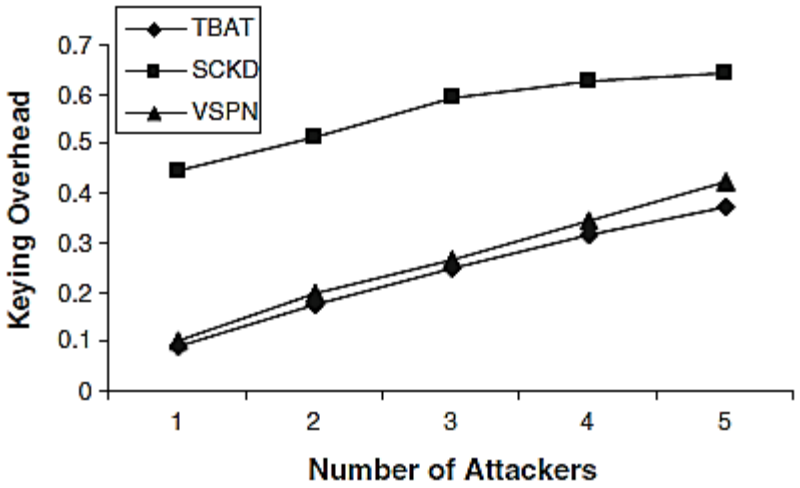


Figure 7: Attackers verus keying overhead

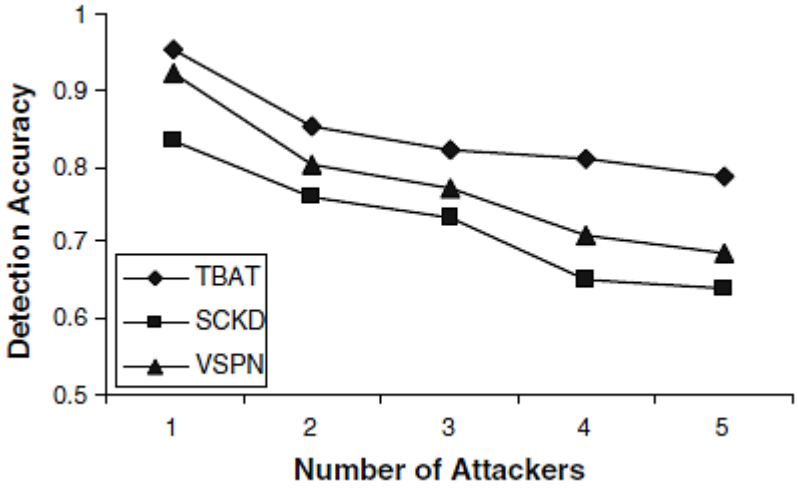


Figure 8: Attackers versus detection accuracy

Table Number of clusters for various ranges

Range	Number of clusters per lane	Number of nodes per cluster
250	3	12
300	3	12

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

350	2	18
400	2	18

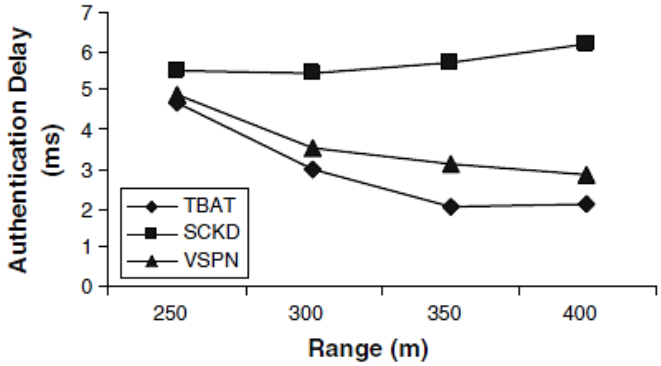


Figure 9: Range verus authentication delay

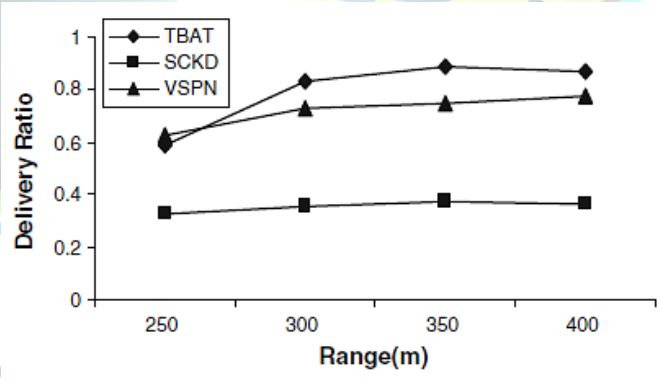


Figure 10: Range verus delivery ratio

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

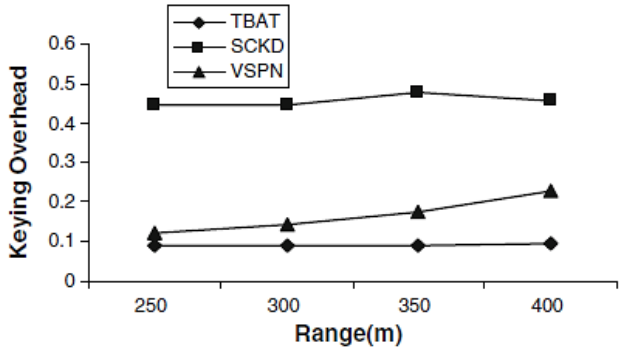


Figure 11: Range verus overhead

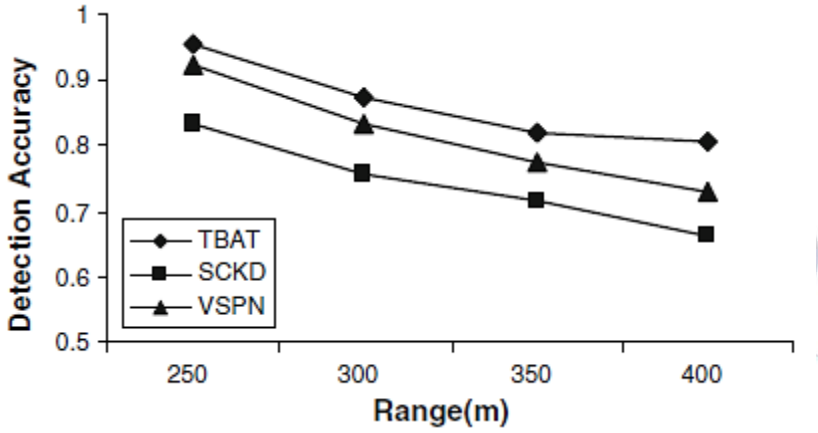


Figure 12: Range verus Detection accuracy

5. Conclusion

In our paper we developed a threshold based authentication scheme for cluster based VANETs. For that, the vehiclesare clustered and the threshold degree of each node is estimated.The threshold degree is a combination of direct threshold degree andindirect threshold degree. Based on this estimated threshold degree,the cluster heads (CH) are selected. Then each vehicle ismonitored by a set of verifiers. Then we add digital signatureto the messages signed by the sender and encryptedusing a public/private key as distributed by a trustauthority and decrypted by the destination. This verifies theidentity

of sender as well as receiver thus providing authentication to the scheme. Simulation results show thatthe proposed technique reduces the authentication delayand keying overhead while increasing the packet deliveryratio.

Reference

[1] Network simulator, http://www.isi.edu/nsnam/ns.

[2] Qin, H., Li, Z. Wang, Y., Lu, X., Zhang, W. S., & Wang, G.(2010). An integrated network of roadside sensors and vehiclesfor driving safety: Concept, design and experiments. In IEEEInternational Conference on Pervasive Computing and Communications(PerCom).

[3]Feng, W., Alshaer, H., &Elmirghani, J. M. H. (2010). Greeninformation and communication technology: Energy efficiency ina motorway model. IET Communications, 4(7), 850–860.

[4]Pradeep, B., ManoharaPai, M. M., Boussedjra, M., &Mouzna, J.(2009). Global public key algorithm for secure location service inVANET.In 9th International Conference on Intelligent TransportSystems Telecommunications, (ITST).

[5] Rivas, D. A., Barcelo-Ordinas, J. M., Zapata, M. G., &Morillo-Pozo, J. D. (2011). Security on VANETs: Privacy, misbehavingnodes, false information and secure data aggregation.Journal of Network and Computer Applications, 34(6), 1942–1955.

[6]Nayyar, Z., Khattak, M. A. K., Saqib, N. A., &Rafique, N.(2015). Secure clustering in vehicular ad hoc networks. InternationalJournal of Advanced Computer Science and Applications(IJACSA), 6(9), 285–291.

[7]Feng, W., &Elmirghani, J. M. H. (2009). Green ICT: Energyefficiency in a motorway model. In Third International Conferenceon Next Generation Mobile Applications, Services andTechnologies.

[8]Plo¨ ßl, Klaus, &Federrath, Hannes. (2008). A privacy aware andefficient security infrastructure for vehicular ad hoc networks.Computer Standards and Interfaces, 30, 390–397.

[9]Mokhtara, Bassem, &Azab, Mohamed. (2015). Survey onsecurity issues in vehicular ad hoc networks. Alexandria EngineeringJournal, 54(4), 1115–1126.

[10]Qian, Y., &Moayeri, N. (2008). Design secure and applicationorientedVANET. In IEEE Vehicular Technology Conference,VTC Spring.

[11]Fathian, M., &Jafarian-Moghaddam, A. R. (2015). New clusteringalgorithms for vehicular ad-hoc network in a highwaycommunication environment. Wireless Networks, 21(8),2765–2780.

[12]Daeinabi, A., &Rahbar, A. G. (2013). An advanced securityscheme based on clustering and key distribution in vehicular adhocnetworks. Computers and Electrical Engineering.

[13]Gan˜a´n, C., Mun˜oz, J. L., Esparza, O., Mata-Dı´az, J., &Alins, J.(2014). PPREM: Privacy preserving REvocation mechanism forvehicular ad hoc networks. Computer Standards and Interfaces,36, 513–523.

[14] Zhizhong, J., Chuanhe, H., Liya, X., Bo, W., Xi, C., &Xiying, F. (2012). A trusted opportunistic routing algorithm for VANET.InIEEE Third International Conference on In Networking and Distributed Computing (ICNDC), pp. 86–90.

[15] Chen, T., Mehani, O., &Boreli, R. (2009). Trusted routing for VANET.In IEEE 9th International Conference on IntelligentTransport Systems Telecommunications, (ITST).

[16] Chim, T. W., Yiu, S. M., Hui, L. C. K., & Li, V. O. K. (2014). VSPN: VANET-based secure and privacy-preserving navigation.IEEE Transactions on Computers, 63(2), 1–14.

ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com

International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 5, Special Issue 12, April 2018

[17] Barba, C. T., Aguiar, L. U., Igartua, M. A., Parra-Arnau, J., Rebollo-Monedero, D., Forne´, J., et al. (2013). A collaborativeprotocol for anonymous reporting in vehicular ad hoc networks.Computer Standards and Interfaces, 36, 188–197.