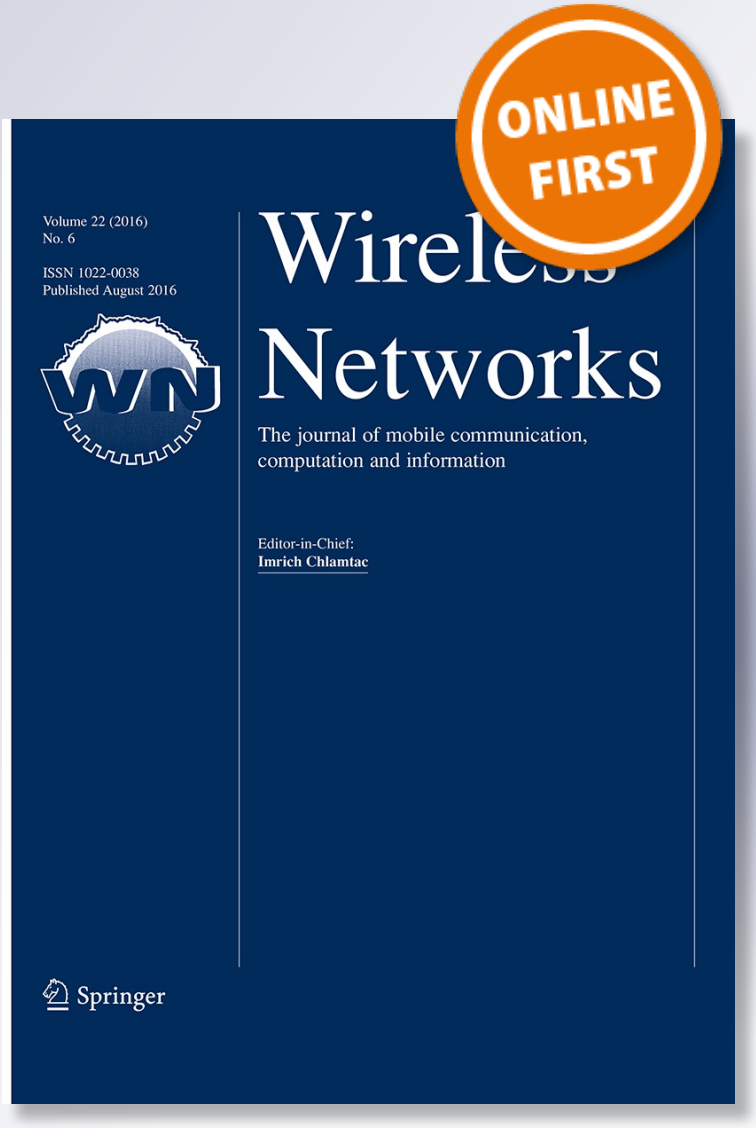
Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)

R. Sugumar, A. Rengarajan & C. Jayakumar

Wireless Networks
The Journal of Mobile Communication, Computation and Information

ISSN 1022-0038

Wireless Netw
DOI 10.1007/s11276-016-1336-6



Springer

Wireless Netw
DOI 10.1007/s11276-016-1336-6

Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)

R. Sugumar[1] · A. Rengarajan[2] · C. Jayakumar[3]

Abstract Since Vehicular ad hoc networks (VANETs) are vulnerable to various kinds of attacks, there is a need to fulfill the security requirements like message privacy, integrity, and authentication. The authentication technique is said to be efficient if it detects compromised nodes accurately with less complexity, reduced authentication delay, and keying overhead. In this paper, a trust-based authentication scheme for cluster-based VANETs is proposed. The vehicles are clustered, and the trust degree of each node is estimated. The trust degree is a combination of direct trust degree and indirect trust degree. Based on this estimated trust degree, cluster heads are selected. Then, each vehicle is monitored by a set of verifiers, and the messages are digitally signed by the sender and encrypted using a public/ private key as distributed by a trusted authority and decrypted by the destination. This verifies the identity of sender as well as receiver thus providing authentication to the scheme. By simulation results, we prove that the proposed technique provides high security with less overhead and delay.

Keywords Vehicular ad hoc networks · Clustering · Trust · Authentication · Trusted authority · Monitoring

✉ R. Sugumar
dr.sugumar16@gmail.com

[1] Department of Computer Science and Engineering, Velammal Institute of Technology, Chennai, India

[2] Department of Computer Science and Engineering, Veltech Multitech SRS Engineering College, Chennai, India

[3] Department of Computer Science and Engineering, Sri Venketeswara College of Engineering, Chennai, Tamil Nadu, India

1 Introduction

VANET is made up of extremely mobile automobiles with sparingly installed stations at the sides of the road; all of them provided with gadgets as well as sensing devices in some cases, that communicate wirelessly. By making use of vehicle-to-vehicle (V2V) ad hoc mode as well as between vehicles and roadside stations by means of vehicle-to-road (V2R) or vehicle-to infrastructure (V2I) communication mode through a base station (BS) or access point (AP), wireless communication can be achieved. For this communication to take place, the AP is usually deployed down the road contained by the BS or AP range for transmission [1]. On board units (OBUs) are deployed on these automobiles in order to enable them and the units along the road, comprising the infrastructure connecting the vehicular network to the central unit. VANET facilitates data transmission such as messages indicating caution related to road situation, traffic condition, and driving condition of the drivers. Application of VANET include accumulating, processing, allocating and delivering the information 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 in delivering unicast communication among vehicles itself or between vehicles and the concerned infrastructure [4, 6].

With the increase in distance, the energy required to provide good quality communication also increases. As a result, the overall energy consumed by the transceiver will be high. On the basis of the number of the relaying nodes and transmission distance between every pair of nodes, the energy consumed increases during communication in multi-hop VANET. Therefore, the energy required for a single transmission amplifies nonlinearly, in the case of little hops and higher transmission distances. So, to obtain

Published online: 29 July 2016

the best energy efficiency, we need to maintain a tradeoff between the hop number and the transmission range for every hop [3, 7].

The target of VANET is achieving higher level of safety on the road. In order to achieve it, every vehicle working as a sensor sends information to each other like warnings related to the present speed, physical location and ESP activity, which lets the drivers to take appropriate measures in case of hazardous condition like accidents, traffic problem, and glaze. Also, official vehicles used by the police and the firefighters can make use of it to transfer messages for stopping other vehicles or clearing the road. Moreover, services on the basis of location and Internet along the road can be provided by VANET. With regard to the protection concerns, reliability, privacy, and accessibility that are the safety and confidentiality requirement, it is required for the three application divisions like warnings and telematics information, alarm signals and instructions, and value-added services. There is a need of a secure topology maintaining trust and allowing cryptography process [8, 9]. Jamming, impersonation, privacy violation, forgery, in-transit traffic tampering, onboard tampering, and so forth are the situations to which VANETs are vulnerable. Therefore, there is a need for VANET to fulfill the security requirements like message privacy and integrity, message non negation, unit validation, admission management, secrecy, accessibility, and responsibility identification [10, 11].

1.1 Problem identification

Achieving energy proficiency as well as security is a challenge in VANET. With the help of cryptographic theory [4], signature using cryptography [12], privacy preservation [13], trust models [14, 15], anonymous credential [16], and collaborative protocol [17], the works [4, 12–17] have guaranteed secure networks. But, certain issues still exist in the current network such as power consumption [3], incapacity to discover compromised nodes [4], complexity [12], message dropping [13], higher delay [14], overhead [15], and collision [17].

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

The paper is organized as follows. Section 2 describes the related works and Sect. 3 provides the detailed explanation of the proposed work. Section 4 explains the simulation results. Finally, Sect. 5 concludes the work.

2 Literature review

Pradeep et al. [4] have presented an algorithm for location service in VANETs based on bilinear coupling cryptography theory. A proficient solution for the network safety was developed by using the electronic signature and applying encryption mechanism on every location service packets and also network layer packets, by not interfering in the fundamental process of location service. This mechanism attained lower signature size by not having to compromise on authenticity of the message. But, this work failed to discover malicious nodes.

Daeinabi and Rahbar [12] have presented an advanced secure mechanism on the basis of clustering and key distribution (SCKD) between members and cluster-heads in VANET. The SCKD is synchronization based algorithm which installed clusters and, the selection of the cluster head is made by the trustworthy nodes. This mechanism makes use of the proxy signature, hashed message authentication code, and symmetric cryptography. But, it is very complicated.

Gañán et al. [13] presented a privacy-preserving revocation mechanism (PPREM) based on the universal one-way accumulator delivering information that is unambiguous, brief, authenticated and unforgeable related to the revoking status of every certificate as it maintains the confidentiality of the user nodes. But, there are possibilities of the message being dropped in the first few stages.

Zhizhong et al. [14] have presented a trust model based on trust degree and executed on opportunistic routing. In every node, the trust relation with the surrounding nodes and also the trust degree were determined. But, this technique had increased average delay.

Chim et al. [16] presented a navigation mechanism which uses the online road information gathered by a vehicular ad hoc network (VANET), which lets the drivers towards the required destination in the real time method as well as in the distributed format. There is guarantee of driver privacy, which is attained by the queries made by the destination and the driver that offers the query that cannot be connected to any of the nodes, which includes even the authenticated nodes. This was attained by the use of an unsigned record. But, this mechanism was unscalable.

Chen et al. [15] have presented a trusted routing framework to ensure message authentication, node-to-node

trust, and rout ability authentication, without any of the online aid from the Certificate Authorities (CA). The aim of this mechanism was to allow route validation, instead of simply safeguarding the messages related to routing protocol or even authorizing nodes. But, this mechanism faced the overhead issue.

Barba et al. [17] have presented a new collaborative protocol for implementing anonymity in multi-hop VANETs. It is done on the basis of a forwarding probability to verify that the next forwarding step in message routing is arbitrary or based on the routing protocol. But, due to flipside buffering, the number of collision rises.

3 Trust based authentication technique

3.1 Overview

In this paper, we propose to develop a trust based authentication scheme for cluster based VANETs. In this scheme the vehicles are clustered [12] and the trust degree of each node is estimated. The trust degree is a combination of direct trust degree and indirect trust degree. Direct trust degree of node is calculated from neighbors using past interactions whereas indirect trust degree is recommendation trust degree from the most similar nearest neighbors. Based on this estimated trust degree, the cluster heads (CH) are selected. Then each vehicle is monitored by a set of verifiers. Then we add digital signature to the messages signed by the sender and encrypted using a public/ private key as distributed by a trusted authority and decrypted by the destination. This verifies the identity of sender as well as receiver thus providing authentication to the scheme.

Figure 1 shows the block diagram of the proposed trust based authentication scheme for clustered VANET.

3.2 Adversarial model

The attacks in VANET are of two types. They are active attack and passive attack. In a passive attack, the attacker eavesdrops but does not modify the message, whereas in an active attack, the attacker may transmit messages, replay old messages, modify messages in transit, or delete selected messages. Man-in-the-middle and replay attacks are considered in the proposed work. Man-in-the-middle attack is an active attack in which the attacker secretly relays and alters the communication between two parties who believe that they are directly communicating with each other. Replay attack is also an active attack in which the attacker may repeat the data or delay the data. Node-to-node authentication (described below) is used to address these attacks (Fig. 2).

3.3 Clustering of vehicles

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

Initially the vehicles are divided into several clusters in a highway environment with two bands and each band having three lanes. Each cluster consists of one cluster head (CH) and one or more members. Vehicles in one cluster are linked directly and vehicles that are located in two different clusters can communicate together via their CHs. Each vehicle can play the role of a CH or gateway or member. If one vehicle is located within two or more clusters, it is called a gateway. Each CH maintains the information about its members and gateways.

The cluster head election process is described in Algorithm 1.

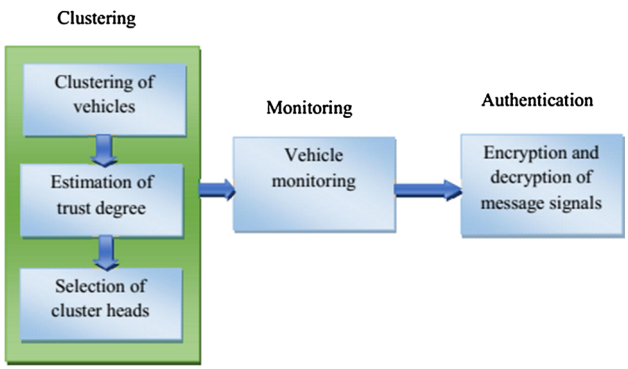


Fig. 1 Block diagram of trust based authentication scheme

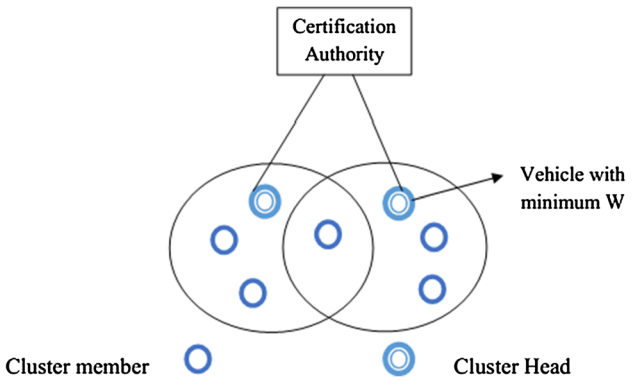


Fig. 2 Cluster formation and CH selection

Algorithm 1

Notations	
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 of* V_j
D_{ij}	*Distance between* V_j *and* V_i
NV_j	*Number of neighbors of* V_j
R	*Dynamic transmission range*
θ	*Direction of vehicle*
S	*Speed of vehicle*
DTr	*Trust degree*
$\alpha, \beta, \delta, \gamma, \eta$	*Weighting Constants*

1. Each vehicle V_i declares itself as a CH and broadcast the beacon $B[Add_i, Id_i]$
2. Each vehicle V_j creates Nl_j after receiving $B[Add_i, Id_i]$ from each V_i
3. Then V_j estimates D_{ij}
4. V_j calculates a weighted sum

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

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 these parameters, the CH which is selected based on it will be trustiest and efficient.

5. Then V_k with W_k = Minimum is selected as CH.

3.4 Estimation of trust degree

Trust degree estimation is done for the selection of Cluster Heads (CH). Trust relationships made from the direct interactions is described as direct trust. The trust relationship built from the trusted node or the chain of trusted node is called as indirect trust node [14].

The direct trust degree from vehicle p to vehicle q is given by,

$$T^d_{new}(p,q) = \begin{cases} T^d_{old}(p,q) + RF, (ST > 0) \\ T^d_{old}(p,q) - PF, (FT > 0) \end{cases} \quad (2)$$

where

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

RF—Reward factor,

PF—Penalty factor,

ST, FT—Number of successful and failed transactions between T_{old} and T_{new} in time interval Δt

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

$$T^r_{(p.q)} = \frac{\sum_{k \in m} T^d(k,q) * s(p,k)}{\sum_{k \in m} s(p,k)} \quad (3)$$

K—common neighbor vehicle

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

m—number of most similar nearest-neighbors of p and q.

The estimation of trust degree is the sum of direct trust and indirect trust,

$$T(p,q) = \alpha \times T^d(p,q) + \beta \times T^r(p,q) \quad (4)$$

α and β—weighing factors for $T^d(p,q)$ and $T^r(p,q)$

The steps involved in the estimation of total trust degree is illustrated in Algorithm 2

Algorithm 2

Notations	
T(p,q)	*Trust degree between vehicles p and q*
N(p)	*Neighbor of node p*
T^d	*Direct trust degree*
T^r	*Indirect trust degree*
tc	*Current time*

1. Node p collects the local topology information.
2. T^d is calculated by p based on the neighbor table and historical events with N(p) using (2)
3. If there is no interaction between the p and q, then
4. T (p, q)= T^d .
5. Store T^d and tc in local information table
6. End if
7. If there is interaction between p and q, then
8. Update T^d .
9. T^r is calculated by p by estimating similar T^d values of N(p) to q, using (3)
10. Calculate T(p, q) using (4)
11. End if

3.5 Vehicle monitoring

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

vehicle monitoring process are illustrated in Algorithm 3 and in Fig. 3.

Algorithm 3

Notations	
T_{min}	*Minimum threshold value of trust degree*
$T(V_j)$	*Total trust degree of vehicle* V_j
CA	*Certificate Authority*
RSU	*Road Side Unit*

1. $\{V_i\}$ detect the abnormal behaviors of vehicle V_j by monitoring, when V_j acts as a relay node or source node.
2. After detecting abnormal behavior of V_j, the CH requests for the trust degree of V_j from other verifiers in the cluster.
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.
4. All other cluster members updates their neighbor table based on the new value of $T(V_j)$.
5. If new $T(V_j) >= T_{min}$, then

All other cluster members cooperate with V_j.

6. Else
7. CH informs the id of V_j to the CA.
8. CA broadcasts the ID of V_j to all the vehicles and RSUs.
9. End if

Note The behavior of a CH will also be monitored by other trustier vehicles of the cluster. When the CH exhibits abnormal behaviors, a new CH should be selected for the cluster

3.6 Node-to-node authentication

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

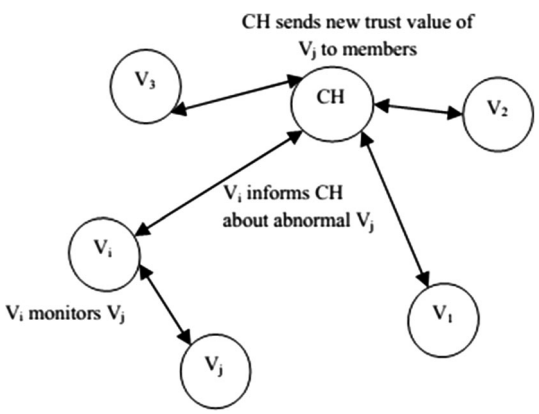


Fig. 3 Vehicle monitoring

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

The below figure shows the node-to-node authentication process (Fig. 4).

3.7 Steps involved in trust based authentication

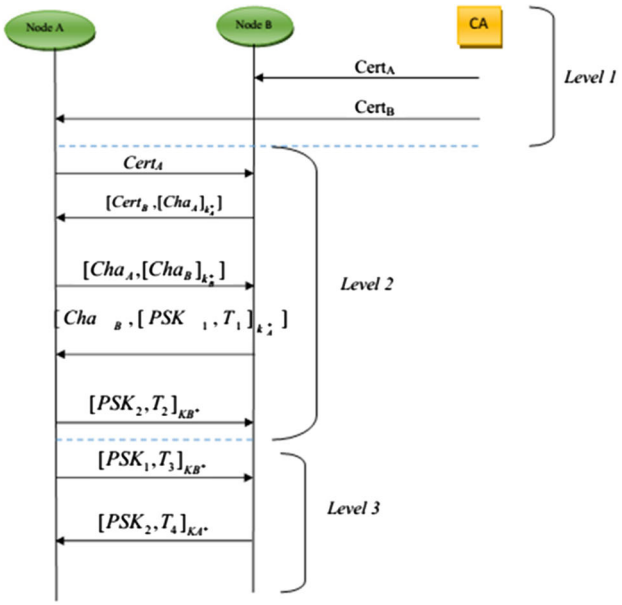
The entire steps involved in the trust based authentication technique can be summarized as:

(a) Initially the vehicles are clustered.
(b) Trust degree of each node is estimated based on direct and indirect trust degrees.
(c) In each cluster, cluster head is selected based on the weighted sum.
(d) Vehicles are monitored by a set of verifiers in each cluster.
(e) The trust degrees of vehicles with abnormal behavior are checked by CH.
(f) Abnormal nodes with least trust degree are isolated by the CA.
(g) In node to node authentication, a digital signature is added to the messages signed by the sender and encrypted using a public/ private key as distributed by a trusted authority and decrypted by the destination.
(h) The sender signs the message using the private key and the receiver verifiers the message with the signer's public key.
(i) At the end of the handshake, two nodes exchange secret keys for quick re-association in the future.

4 Simulation results

4.1 Simulation model and parameters

We use NS-2 [17] to simulate our proposed Trust based Authentication Technique (TBAT) for clustered VANET. Figure 5 shows the simulation topology. It consists of two bands with each band consisting 3 lanes. The cluster head



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
$PSK_i - Session\ share\ key$	$T_i - Timestamp$

Fig. 4 Node-to-node authentication

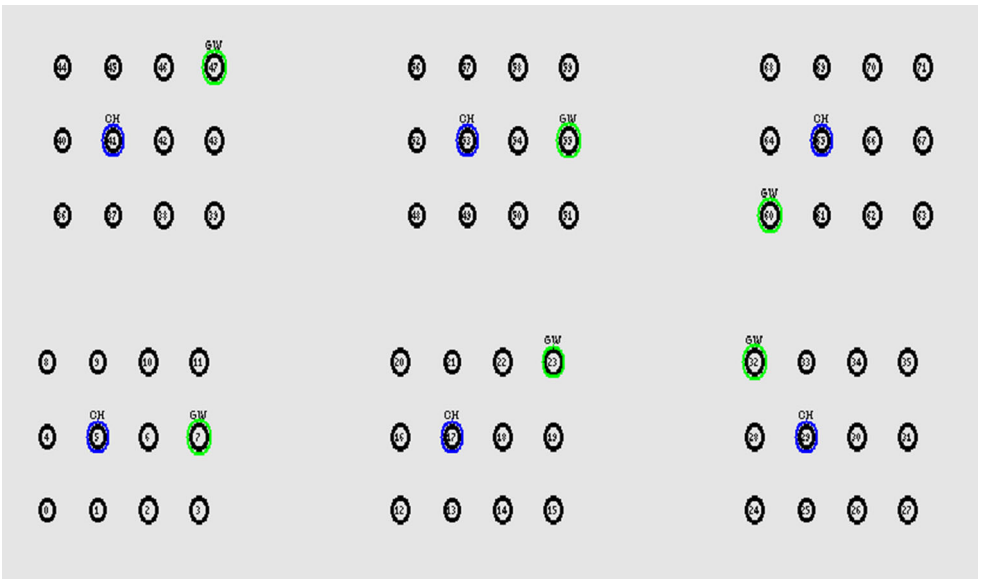


Fig. 5 Simulation topology

and gateway nodes are marked as blue and red colors, respectively.

Our simulation settings and parameters are summarized in Table 1. We compare TBAT with Secure scheme based on Clustering and Key Distribution (SCKD) [12] and VSPN [16]. The performance is evaluated in terms of packet delivery ratio, authentication delay, keying overhead and detection accuracy.

Table 1 Simulation settings

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

5 Results

5.1 Varying the attackers

In this experiment, the transmission range is fixed as 250. There are totally 3 clusters formed in each lane with 12 members per cluster. The number of malicious nodes or attackers is varied from 1 to 5 in each cluster.

Figure 6 shows the authentication delay for all the techniques when the attackers are increased. When the number of attackers is increased from 1 to 5, the time involved in trust estimation and authentication increases, leading to the increase in delay. Since TBAT does not involve time consuming key generation and related cryptographic operations, the authentication delay is less by 22 % when compared to SCKD which involves key generation proxy signature operations. When compared to VSPN, the delay of TBAT is 4 % less.

Figure 7 shows the packet delivery ratio for all the techniques when the attackers are increased. When the number of attackers is increased, more packets will be dropped, leading to the decrease in packet delivery ratio. The trust estimation method in TBAT is more effective than SCKD, since it considers both direct and indirect trust values. Moreover, the certificate based authentication technique of TBAT isolates more attackers. So the delivery ratio of TBAT is 46 % higher than SCKD and 8 % higher than VSPN.

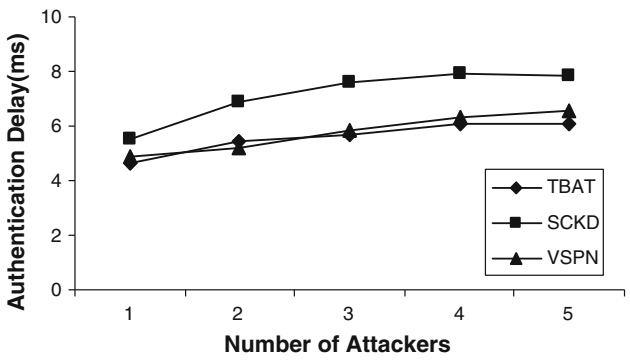


Fig. 6 Attackers versus authentication delay

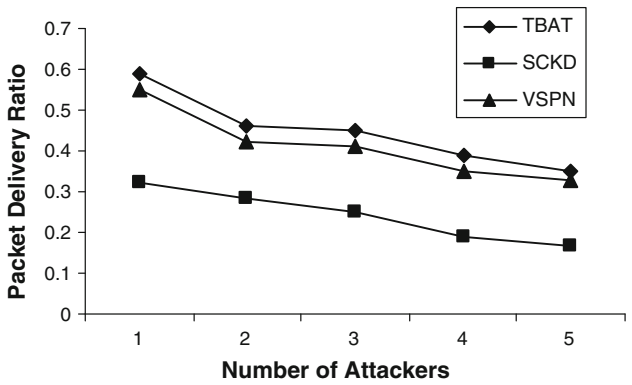


Fig. 7 Attackers versus delivery ratio

Figure 8 shows the keying overhead occurred for all the techniques when the attackers are increased. Since TBAT does not involve complex key generation and related cryptographic operations, the keying overhead is less by 61 % when compared to SCKD which involves key generation proxy signature operations. The keying overhead of TBAT is 10 % less, when compared to VSPN.

Figure 9 shows the detection accuracy for all the 3 techniques when the attackers are increased. When the number of attackers is increased, detection accuracy of all the 3 schemes decreases. The trust estimation method in TBAT is more effective than SCKD, since it considers both direct and indirect trust values. So the detection accuracy of TBAT is 14 % more than SCKD and 8 % more than VSPN.

5.2 Based on transmission range

In the next experiment, in order to evaluate the effect clustering on transmission range, the range is varied as 250, 300, 350, and 400 m. Table 2 shows the number of clusters formed and its size, when the range is increased from 250

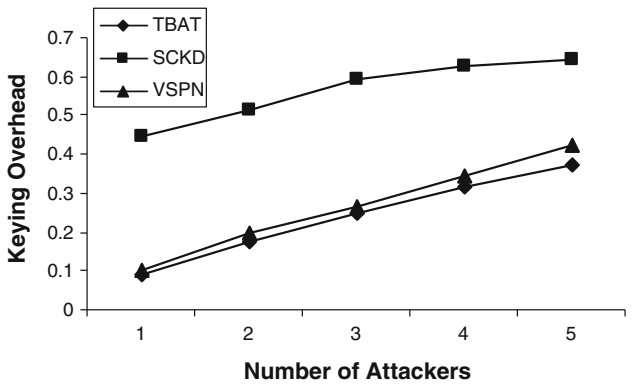


Fig. 8 Attackers versus keying overhead

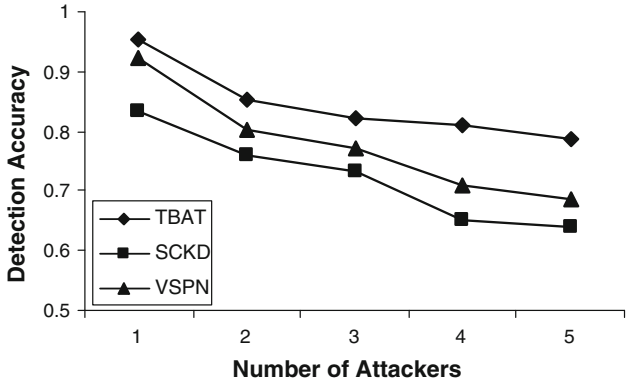


Fig. 9 Attackers versus detection accuracy

Table 2 Number of clusters for various ranges

Range	Number of clusters Per Lane	Number of nodes per Cluster
250	3	12
300	3	12
350	2	18
400	2	18

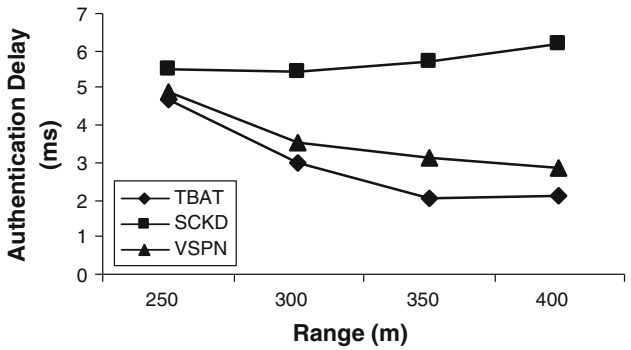


Fig. 10 Range versus authentication delay

to 400 m. The number of clusters formed decreases as the range increases, since more number of nodes are covered in higher transmission ranges. The number of attackers per cluster is kept as 2.

Figures 10, 11, 12 and 13 show the results of authentication delay, delivery ratio, keying overhead and detection accuracy for all the 3 techniques by varying the range as 250, 300, 350, and 400 m. As described in the previous set of results, when comparing the performance of the 3 techniques, we infer that TBAT outperforms SCKD and VSPN by 48 and 20 % in terms of delay, 54 and 8 % in terms of delivery ratio, 80 and 41 % in terms of overhead and 14 and 5 % in terms of accuracy.

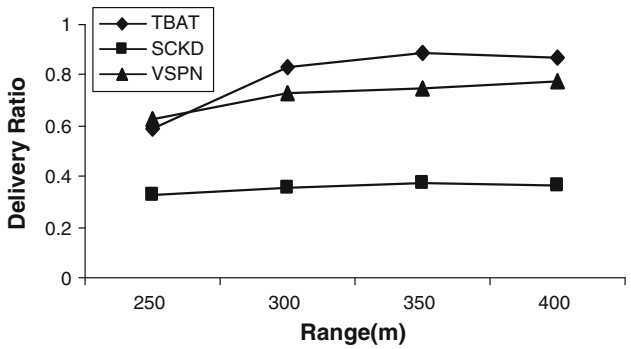


Fig. 11 Range versus delivery ratio

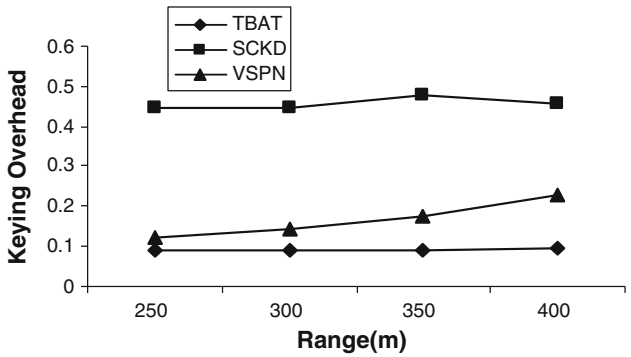


Fig. 12 Range versus overhead

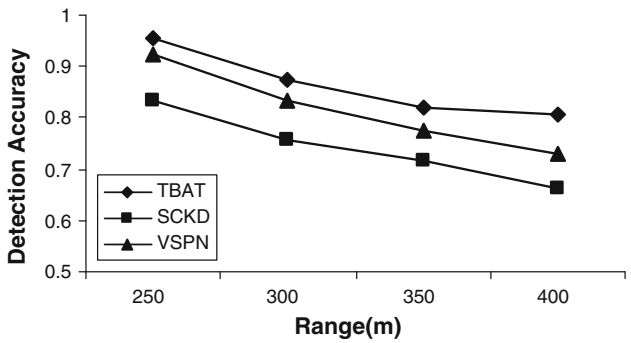


Fig. 13 Range versus detection accuracy

6 Conclusion

In our paper we developed a trust based authentication scheme for cluster based VANETs. For that, the vehicles are clustered and the trust degree of each node is estimated. The trust degree is a combination of direct trust degree and indirect trust degree. Based on this estimated trust degree, the cluster heads (CH) are selected. Then each vehicle is monitored by a set of verifiers. Then we add digital signature to the messages signed by the sender and encrypted using a public/private key as distributed by a trusted authority and decrypted by the destination. This verifies the

identity of sender as well as receiver thus providing authentication to the scheme. Simulation results show that the proposed technique reduces the authentication delay and keying overhead while increasing the packet delivery ratio.

References

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 vehicles for driving safety: Concept, design and experiments. In *IEEE International Conference on Pervasive Computing and Communications (PerCom)*.
3. Feng, W., Alshaer, H., & Elmirghani, J. M. H. (2010). Green information and communication technology: Energy efficiency in a motorway model. *IET Communications*, *4*(7), 850–860.
4. Pradeep, B., Manohara Pai, M. M., Boussedjra, M., & Mouzna, J. (2009). Global public key algorithm for secure location service in VANET. In *9th International Conference on Intelligent Transport Systems Telecommunications, (ITST)*.
5. Rivas, D. A., Barcelo-Ordinas, J. M., Zapata, M. G., & Morillo-Pozo, J. D. (2011). Security on VANETs: Privacy, misbehaving nodes, 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. *International Journal of Advanced Computer Science and Applications (IJACSA), 6*(9), 285–291.
7. Feng, W., & Elmirghani, J. M. H. (2009). Green ICT: Energy efficiency in a motorway model. In *Third International Conference on Next Generation Mobile Applications, Services and Technologies*.
8. Plößl, Klaus, & Federrath, Hannes. (2008). A privacy aware and efficient security infrastructure for vehicular ad hoc networks. *Computer Standards and Interfaces, 30*, 390–397.
9. Mokhtara, Bassem, & Azab, Mohamed. (2015). Survey on security issues in vehicular ad hoc networks. *Alexandria Engineering Journal, 54*(4), 1115–1126.
10. Qian, Y., & Moayeri, N. (2008). Design secure and application-oriented VANET. In *IEEE Vehicular Technology Conference, VTC Spring*.
11. Fathian, M., & Jafarian-Moghaddam, A. R. (2015). New clustering algorithms for vehicular ad-hoc network in a highway communication environment. *Wireless Networks, 21*(8), 2765–2780.
12. Daeinabi, A., & Rahbar, A. G. (2013). An advanced security scheme based on clustering and key distribution in vehicular ad-hoc networks. *Computers and Electrical Engineering*.
13. Gañán, C., Muñoz, J. L., Esparza, O., Mata-Díaz, J., & Alins, J. (2014). PPREM: Privacy preserving REvocation mechanism for vehicular 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. In *IEEE 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 Intelligent Transport 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.
17. Barba, C. T., Aguiar, L. U., Igartua, M. A., Parra-Arnau, J., Rebollo-Monedero, D., Forné, J., et al. (2013). A collaborative protocol for anonymous reporting in vehicular ad hoc networks. *Computer Standards and Interfaces, 36*, 188–197.

Dr. R. Sugumar has more than 13 years of teaching and research experience. He received the B. E. degree from the University of Madras, Chennai, India in 2003, M. Tech. degree from Dr. M. G. R. Educational and Research Institute, Chennai, India, in 2007, and the Ph.D. degree in Computer Science and Engineering at from Bharath University, Chennai, India, in 2011. From 2003 to 2016, he has worked at different levels in various reputed engineering colleges across India. He is currently working as an Associate Professor in the Department of Computer Science and Engineering at Velammal Institute of Technology, Chennai, India. His research interests include data mining, cloud computing and networks. He has published more than 30 research articles in various international journals and conference proceedings. He is acting as a reviewer in various national and international journals. He has chaired various international and national conferences. He is a life time member of ISTE and CSI.

Dr. A. Rengarajan received the B.E. degree from the Madurai Kamaraj University, Madurai, India in 2000, the M.E. degree from Sathyabama University, Chennai, India, in 2005, and the Ph.D. degree from Bharath University, Chennai, India, in 2011. From 2000 to 2011, he worked at different levels in various reputed engineering colleges across India. He is currently an Professor in the Department of Computer Science and Engineering at Veltech Multitech Dr.Ranagarajan Dr.Sakunthala Engineering College, Chennai, India. His research interests are in Network Security, Mobile Communication and Data Warehousing and Data Mining. He has published more than 30 research articles in various international journals and conference proceedings. He is acting as a reviewer in various national and international journals. He chaired various International and National Conferences.

Dr. C. Jaykumar has more than 18 years of teaching and research experience. He did his Postgraduate in M.E. in Computer Science and Engineering at College of engineering, Guindy, and Ph.D. in Computer Science and Engineering at Anna University, Chennai. He has Received 25 lakhs Grant from AICTE for RPS Project and Staff Development Program. He guided 5 Ph.D. Students under Anna University Chennai, India, 5 Ph.D. Students under Bharat university, India and two student has submitted thesis under Anna University Chennai. He has published 143 research papers in International Journal, International and National conferences. He has guiding a number of research scholars in the area Adhoc Network, Security in Sensor Networks, Mobile Database and Data Mining under Anna University Chennai, Sathayabama University and Bharathiyar University, Bharath University. He chaired the session at various International Conference, National level Conferences, Staff development Program and workshop. He was Advisor and Technical Committee Member for many International and National Conferences. He has Coordinated National Board of Accreditation, Anna University Affiliation, Anna University Research Nodal Centre, and TCS Accreditation at various colleges. He was the "Anna University Inspection Committee Member" for Affiliated Colleges for the academic year 2008–09. He held the Member position in Board of Studies in Meenakshi University, Chennai, Technical Committee member in SRM University and SRM Arts and Science Chennai. He conducted Various National Conference, Staff Development Program, Workshop, Seminar in associated with Industries like Infosys and TCS. Currently he is working as Professor and HOD in the Department of Computer Science and Engineering, Sri Venketeswara College of Engineering, Tamil Nadu, India.