International Journal of Scientific Research & Engineering Trends
Volume 6, Issue 4, July-Aug-2020, ISSN (Online): 2395-566X

Trust Based Authentication for Vehicular Ad Hoc Networks

Rajendra Thakur , Assistant Prof. Lokesh Parashar
Department of Computer Science,
Patel College of Science & Technology Indore, India
rajendrathakur004@gmal.com, lokesh23324@gmail.com

***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 pro- posed. 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 over head and delay.**

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

I.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 vehi- cle-to-road (V2R) or vehicle-to infrastructure (V2I) com-
munication 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 facili- tates 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 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 Inter- net 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 divi- sions 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, on- board 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 valida-tion, admission management, secrecy, accessibility, and responsibility identification [10, 11].

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 cre-dential [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 distribu- tion 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 expla- nation of the proposed work. Section 4 explains the sim- ulation results. Finally, Sect. 5 concludes the work.

II. LITERATURE REVIEW

Pradeep et al. [4] have presented an algorithm for location service in VANETs based on bilinear coupling cryptogra-phy 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 dis-tribution (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.
Gan˜a´n et al. [13] presented a privacy-preserving revo- cation mechanism (PPREM) based on the universal one- way accumulator delivering information that is unam- biguous, 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 was determined. But, this tech-nique 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)[18], 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 pro- tocol 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 proba-bility 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 collisions rises.

III. TRUST BASED AUTHENTICATION TECHNIQUE

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.

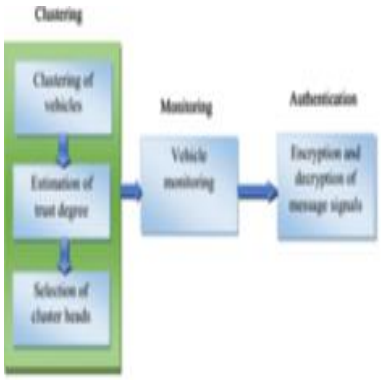


Fig. 1 Block diagram of trust-based authentication scheme

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 selec- ted 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. 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.

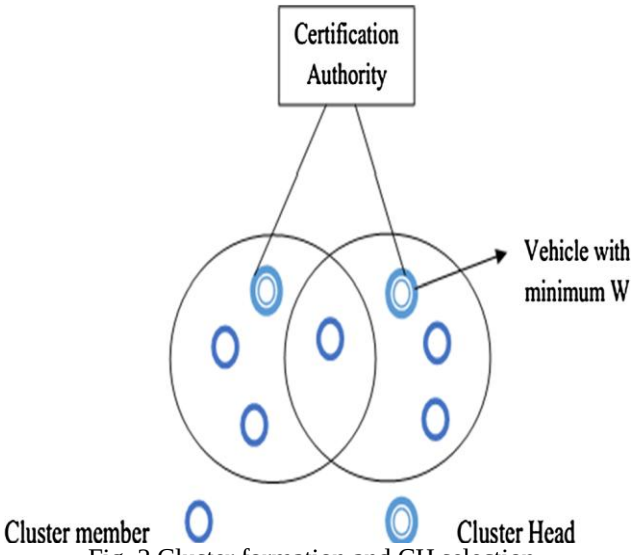


Fig. 2 Cluster formation and CH selection

Algorithm 1 Notation	
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 Neighbor of V_j
R	Dynamic transmissionrange
θ	Direction ofvehicle
S	Speed ofvehicle
DT_r	Trustdegree
α, β, γ, δ, η,	WeightingConstants

- Each vehicle Vi declares itself as a CH and broadcast the beacon B[Addi, Idi]
- Each vehicle Vj creates Nlj after receiving B[Addi, Idi] from each Vi
- Then Vj estimates Dij
- Vj calculates a weighted sum
- $W_j = \alpha NV_j + \beta.R + \delta.\theta + \gamma.S - \eta DT_r$ (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.

- Then Vk with Wk = Minimum is selected as CH

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 relation- ship 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,

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

where
Told = 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 Told and Tnew 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 factor 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

- Nodepcollectsthelocaltopologyinformation.
- T^{d} is calculated by p based on the neighbor table and historical events with N(p) using(2)
- If there is no interaction between the *p* and *q*,then
- T (p, q)= T^{d}.
- StoreT^{d} and tc in local information table
- Endif

Algorithm 2 Notation	
T(p,q)	Trust degree between vehicles pan dq
N(p)	Neighbor of node p
T^{d}	Direct trust degree
T^{r}	Indirect trust degree
tc	Current time

- If there is interaction between *p* and *q*,then

5. Vehicle monitoring

In monitoring phase, a set of verifier nodes collect information about the behavior of all vehicles in a cluster. A vehicle Vi can be a verifier of another vehicle Vj if T(Vi)[T(Vj), where T is the total trust degree stored in the neighbor table of each node. Let Tmin 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 Notation	
T_{min}	Minimum threshold value of trustdegree
$T(V_j)$	Total trust degree of vehicleV_j
CA	CertificateAuthority
RSU	Road SideUnit

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

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

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].

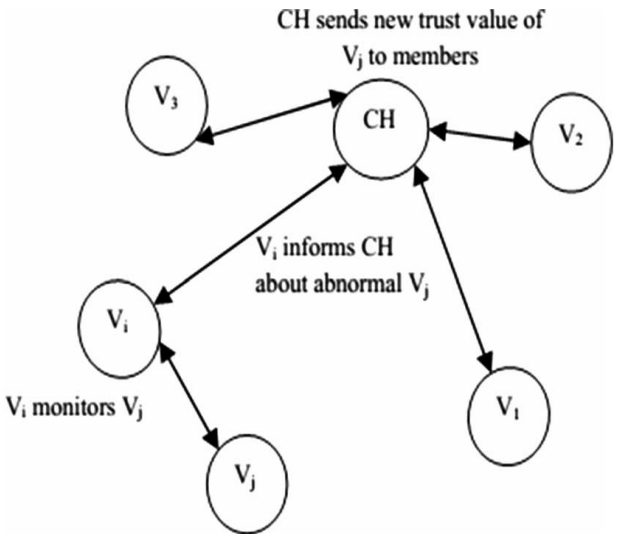


Fig. 3 Vehicle monitoring

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).

Steps involved in trust-based authentication

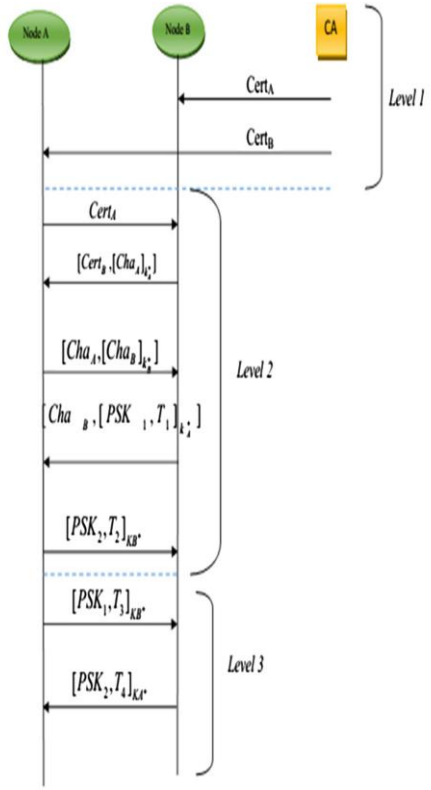
The entire steps involved in the trust-based authentication technique can be summarized as:

- Initially the vehicles are clustered.
- Trust degree of each node is estimated based on direct and indirect trust degrees.
- In each cluster, cluster head is selected based on the weighted sum.
- Vehicles are monitored by a set of verifiers in each cluster.
- The trust degrees of vehicles with abnormal behavior are checked by CH.
- Abnormal nodes with least trust degree are isolated by the CA.
- 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.
- The sender signs the message using the private key and the receiver verifiers the message with the signer's public key.
- At the end of the handshake, two nodes exchange secret keys for quick re-association in the future.

IV. SIMULATION RESULTS

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 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 over- head and detection accuracy.



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.

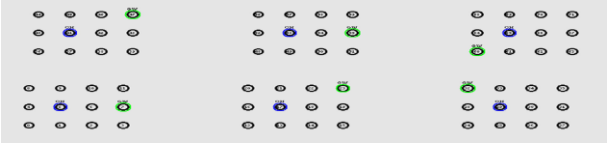


Fig. 5 Simulation topology

Table 1 Simulation settings

Number of nodes	72
AreaSize	2500 x 700m
NumberofBANDS	2
Number of lanes per band	3
Radio range	250,300,350 and 400 m
Simulationtime	50s
Packetsize	512 bytes
Antenna	Omni Antenna

V. RESULTS

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 cryp- tographic operations, the authentication delay is less by 22 % when compared to SCKD which involves key gen- eration proxy signature operations. When compared to VSPN, the delay of TBAT is 4 % less.

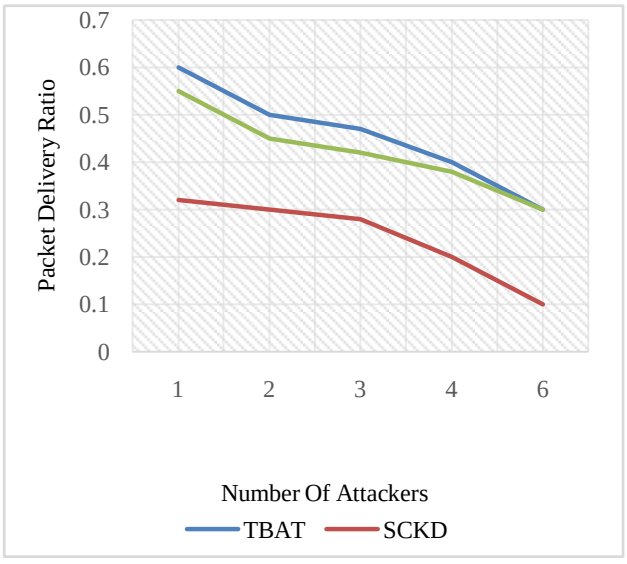


Fig. 6 Attackers versus authentication delay

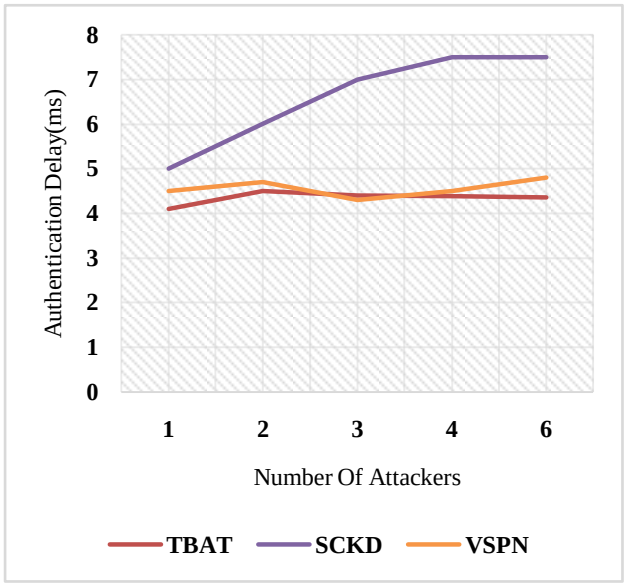


Fig. 7 Attackers versus delivery ratio

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.

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 gen- eration 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.

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 to 400 m. The number of clusters formed decreases as the range increases, since a greater number

of nodes are covered in higher transmission ranges. The number of attackers per cluster is kept as 2.

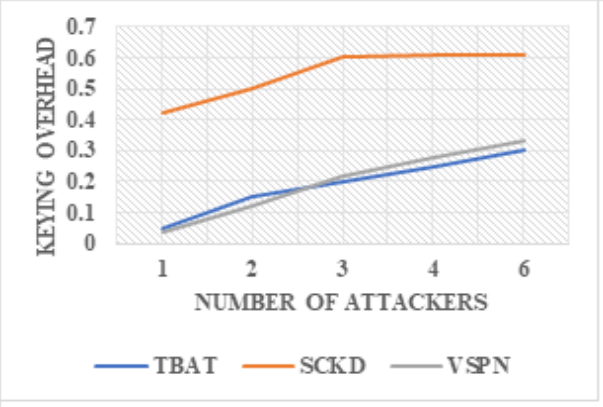


Fig. 8 Attackers versus keying overhead.

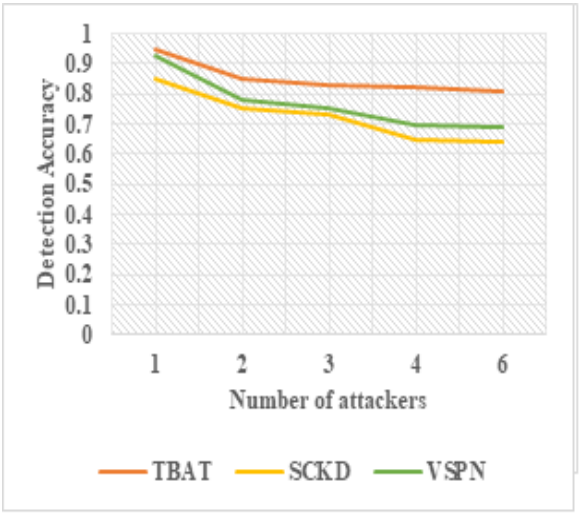


Fig. 9 Attackers versus detection accuracy.

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	5	18
400	2	18

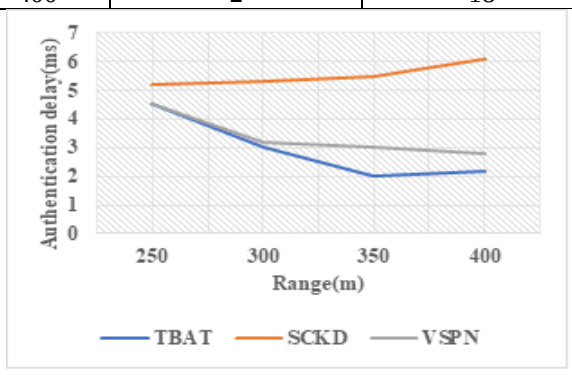


Fig. 10 Range versus authentication delay.

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.

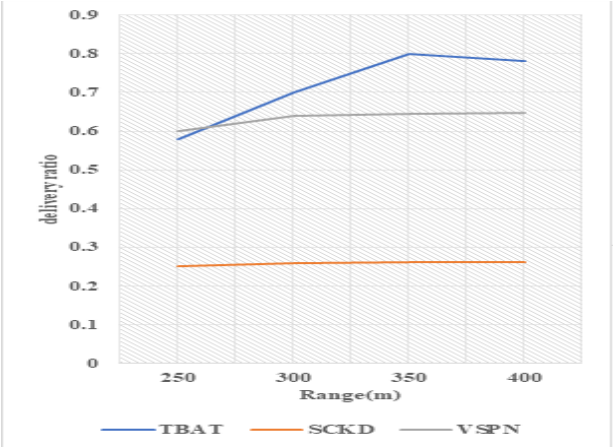


Fig. 11 Range versus delivery ratio.

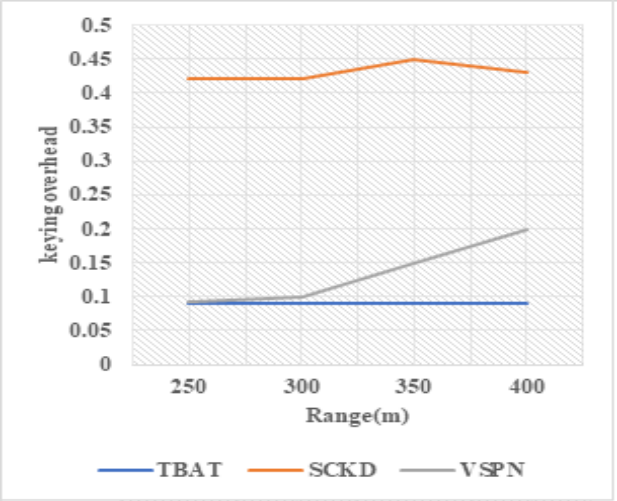


Fig. 12 Range versus overhead.

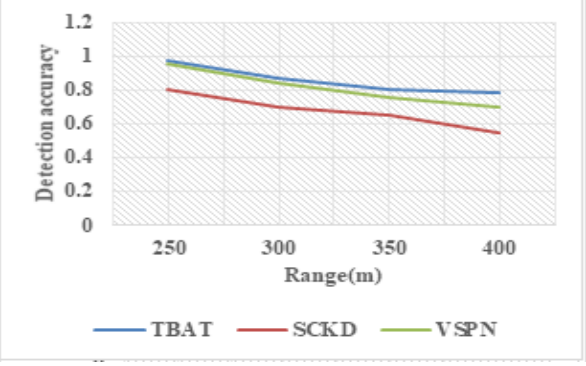


Fig. 13 Range versus detection accuracy.

VI. 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 sig- nature 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 Commu- nications (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 Trans- port Systems Telecommunications, (ITST).
[5] Rivas, D. A., Barcelo-Ordinas, J. M., Zapata, M. G., &Morillo- Pozo, J. D. (2011). Security on VANETs: Privacy, misbehav- ing 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. Interna- tional 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 Confer- ence on Next Generation Mobile Applications, Services and Technologies.
[8] Plo¨ ßl, 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 Engi- neering 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 clus- tering 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] Gan˜a´n, C., Mun˜oz, J. L., Esparza, O., Mata-D´ıaz, J., &Alins, J.
[14] (2014). PPREM: Privacy preserving REvocation mechanism for vehicular ad hoc networks. Computer Standards and Interfaces, 36, 513–523.
[15] 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.
[16] Chen, T., Mehani, O., &Boreli, R. (2009). Trusted routing for VANET. In IEEE 9th International Conference on Intelligent Transport Systems Telecommunications, (ITST).
[17] 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.
[18] Barba, C. T., Aguiar, L. U., Igartua, M. A., Parra-Arnau, J., Rebollo-Monedero, D., Forne´, J., et al. (2013). A collaborative protocol for anonymous reporting in vehicular ad hoc networks. Computer Standards and Interfaces, 36, 188–197.
[19] V. Prakaulya, N. Pareek, and U. Singh, “Network performance in IEEE 802.11 and IEEE 802.11p cluster based on VANET,” in Proceedings of the International Conference on Electronics, Communication and Aerospace Technology, ICECA 2017, 2017, vol. 2017-Janua, doi: 10.1109/ICECA.2017.8212713.