A Threshold Based Authentication Mechanism For Vehicular Ad Hoc Network (Vanet)

Dr. B. Karthikeyan

Assistant Professor, Department of Computer Science, Bishop Heber College (Autonomous) (Affiliated to Bharathidasan University, Tiruchirappalli), Tiruchirappalli, Tamilnadu, India.

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 threshold-based authentication 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 combination of direct threshold degree and indirect threshold degree. Based on this estimated threshold 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 threshold 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 Network, Clustering, Threshold Authentication, Threshold Authority, Monitoring.

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 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 threshold 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].

2.   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], threshold 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, 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 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.

3.   THRESHOLD BASED AUTHENTICATION TECHNIQUE

Aim of this paper is to develop a threshold based authentication scheme for cluster based VANETs. In this scheme the vehicles are clustered [12] and the threshold degree of each node is estimated. The threshold degree is a combination of direct threshold degree and indirect threshold degree. Direct threshold degree of node is calculated from neighbors using past interactions whereas indirect threshold degree is recommendation threshold degree from the most similar nearest neighbors. Based on this estimated threshold 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 threshold authority and decrypted by the destination. This verifies the identity of sender as well as receiver thus providing authentication to the scheme.
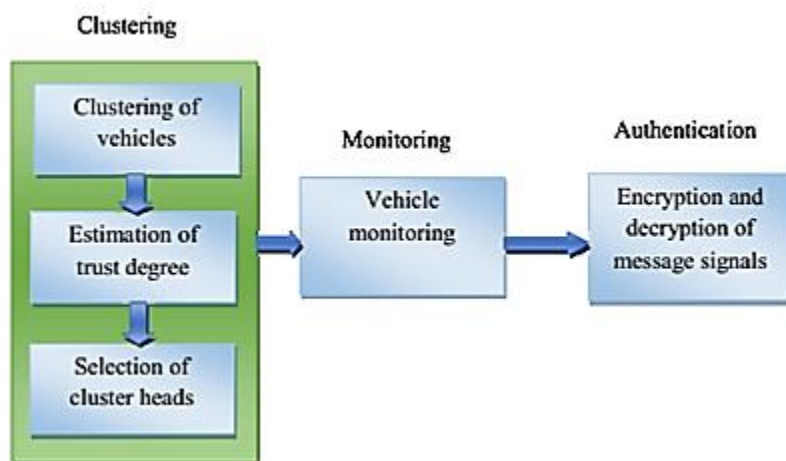

Figure 1: Block Diagram for Threshold based Authentication scheme

3.1   Adversarial Model

The attacks in VANET are of two types. They are active attack and passive attack. In a passive attack, the 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).

3.2   Clustering of Vehicle

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 threshold 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.
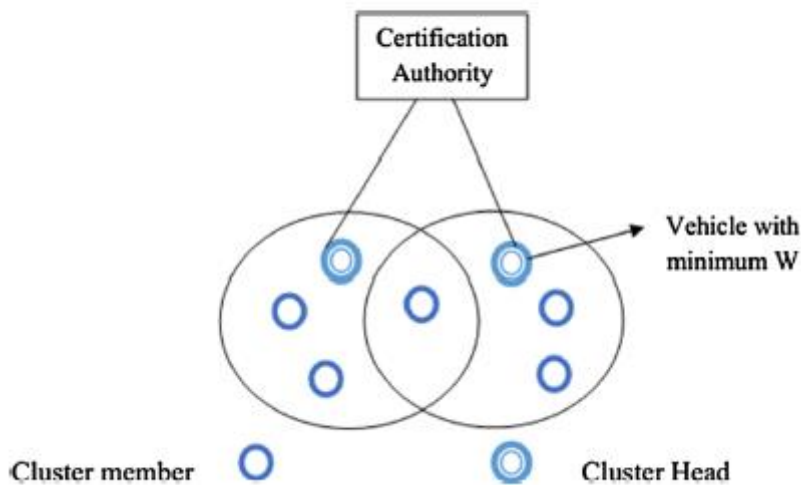

Figure 2: Cluster Formation and Cluster Head Selection

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 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 the vehicle
DTr	Threshold degree
$\alpha, \beta, \delta, \gamma, \eta$	Weighting Constants

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 creates Nl_j after receiving $B[add_i, Id_i]$ from each V_i.

Step 3: Then V_j estimates D_{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 these parameters, the CH which is selected based on it will be threshold and efficient.

Step 5: Then V_k with W_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 direct interactions is described as direct threshold. The threshold relationship built from the trust node or the chain of trust node is 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,

PF—Penalty factor,

ST, FT—Number of successful and failed transactions between T_{old} 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 and q.

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

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

α and β – 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 historical events with N(p) using (2).

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: Update T^d

Step 9: T^r is calculated by p by estimating similar T^d values 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. 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 threshold degree stored in the neighbor table of each node. Let T_{min} be the minimum threshold value of threshold degree. The steps involved in the vehicle 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
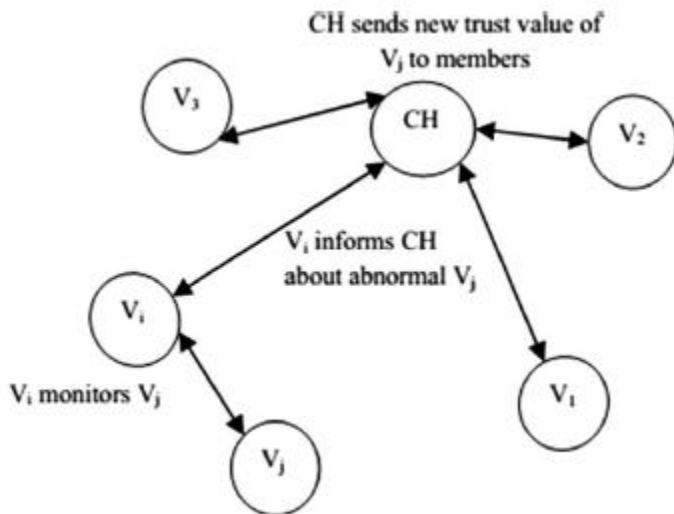
Figure 3: Vehicle Monitoring

Step 1: $\{V_j\}$ detect the abnormal behaviors of vehicle V_j by monitoring, when V_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 $T(V_j) >= T_{min}$, then All 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

3.5 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].

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.
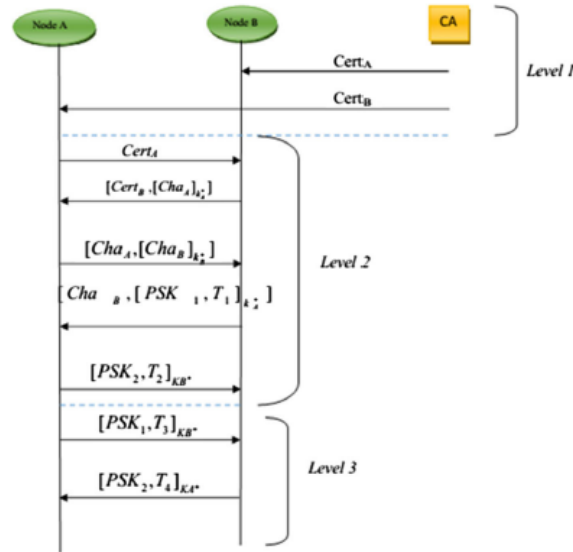
Figure 4: Node to node authentication

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 on direct and indirect threshold 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 threshold degrees of vehicles with abnormal behavior are checked by CH.

(f) Abnormal nodes with least threshold 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 trust 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 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

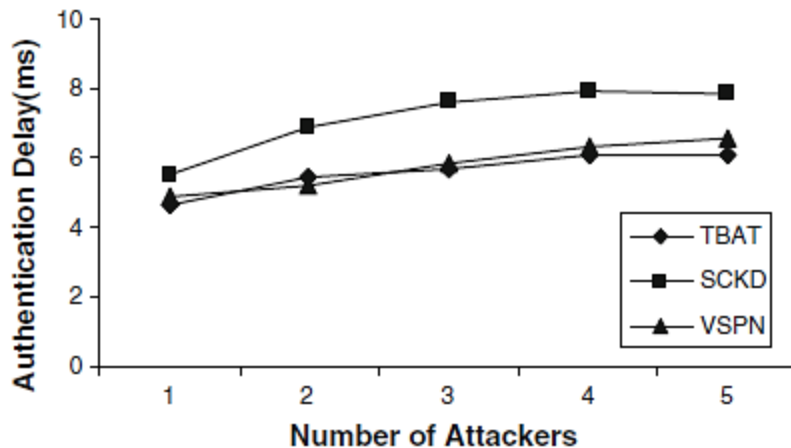|	
Number of nodes	72
Area size	2500 9 700 m
Number of BANDS	2
Number of lanes per band	3
Radio range	250, 300, 350 and 400 m.
Simulation time	50s
Packet size	512 bytes
Antenna	Omni Antenna

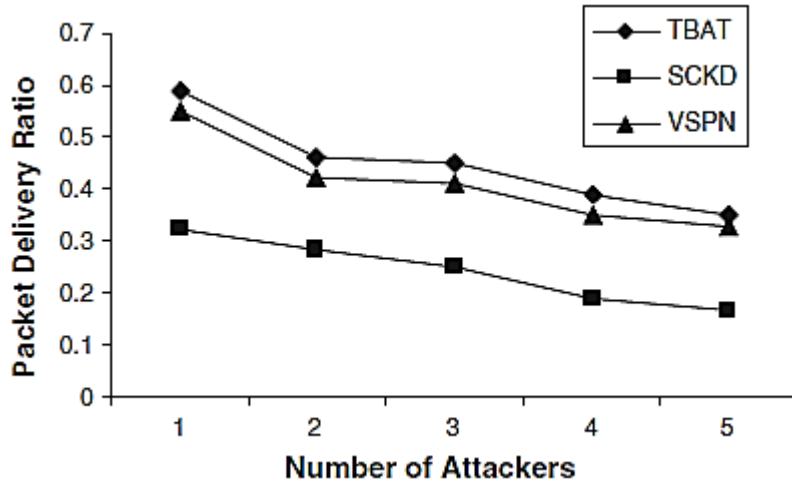**Figure 5: Attackers versus authentication delay**
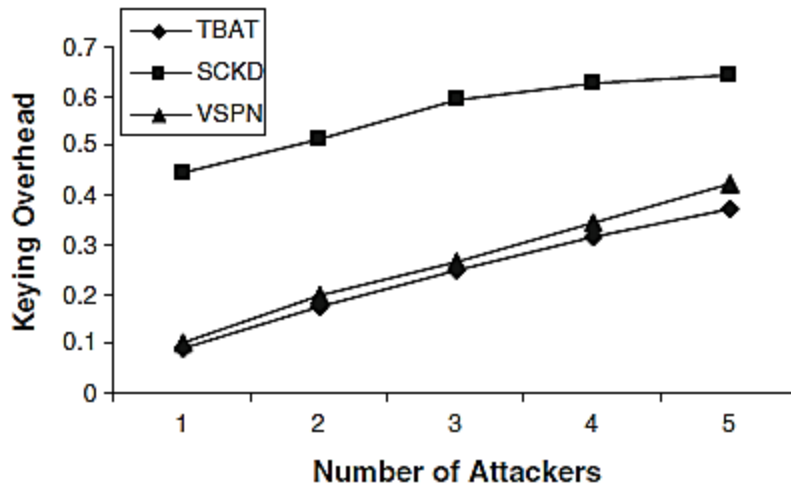
Figure 6: Attackers versus delivery ratio

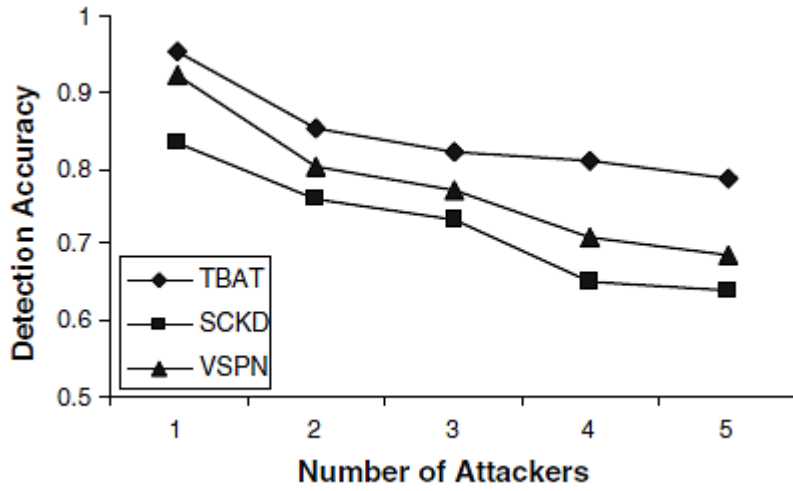**Figure 7: Attackers verus keying overhead**

Figure 8: Attackers versus detection accuracy

Table 5: Number of clusters for various ranges

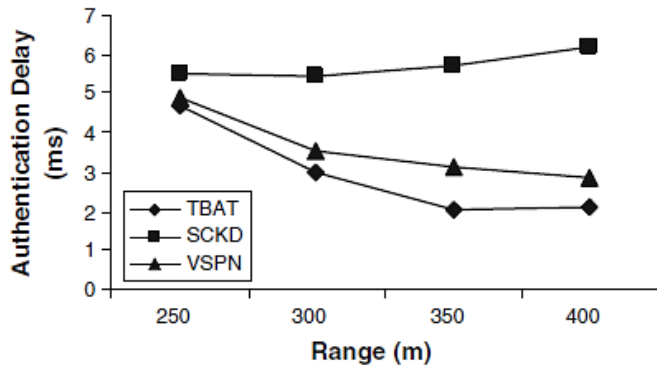| Range	Number of clusters per lane	Number of nodes per cluster
250	3	12
300	3	12
350	2	18
400	2	18

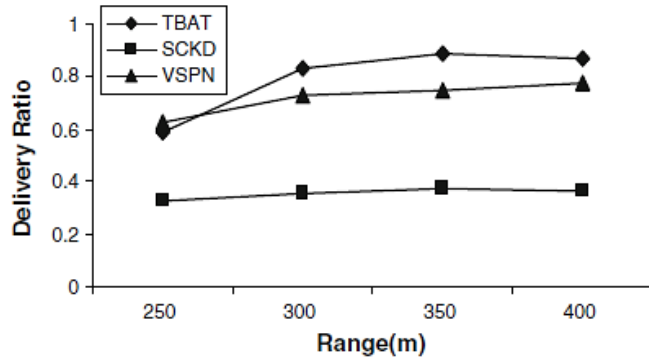**Figure 9: Range verus authentication delay**
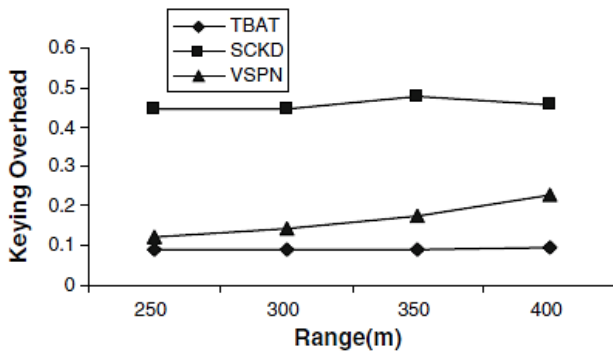
Figure 10: Range verus delivery ratio
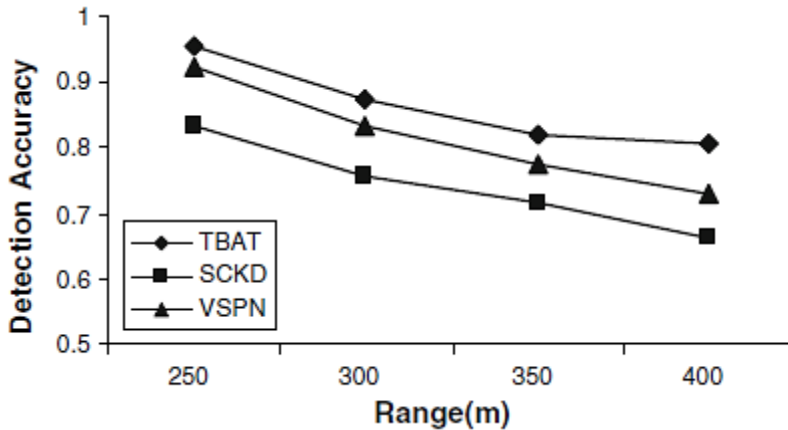
Figure 11: Range verus overhead

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 vehicles are clustered and the threshold degree of each node is

estimated. The threshold degree is a combination of direct threshold degree and indirect threshold degree. Based on this estimated threshold 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 trust 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.

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 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]   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 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 adhoc networks. 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 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., Forne´, J., et al. (2013). A collaborative protocol for anonymous reporting in vehicular ad hoc networks. Computer Standards and Interfaces, 36, 188–197.

[20]   Subhashini, M., & Gopinath, R., Mapreduce Methodology for Elliptical Curve Discrete Logarithmic Problems – Securing Telecom Networks, International Journal of Electrical Engineering and Technology, 11(9), 261-273 (2020).

[21]   Upendran, V., & Gopinath, R., Feature Selection based on Multicriteria Decision Making for Intrusion Detection System, International Journal of Electrical Engineering and Technology, 11(5), 217-226 (2020).

[22]   Upendran, V., & Gopinath, R., Optimization based Classification Technique for Intrusion Detection System, International Journal of Advanced Research in Engineering and Technology, 11(9), 1255-1262 (2020).

[23]   Rethinavalli, S., & Gopinath, R., Botnet Attack Detection in Internet of Things using Optimization Techniques, International Journal of Electrical Engineering and Technology, 11(10), 412-420 (2020).

[24]   Priyadharshini, D., Poornappriya, T.S., & Gopinath, R., A fuzzy MCDM approach for measuring the business impact of employee selection, International Journal of Management (IJM), 11(7), 1769-1775 (2020).

[25]   Poornappriya, T.S., Gopinath, R., Application of Machine Learning Techniques for Improving Learning Disabilities, International Journal of Electrical Engineering and Technology (IJEET), 11(10), 392-402 (2020).