PUF-SecV2X: PUF based Multifactor Authentication and Boundary Forwarder assisted Routing in Secure V2X Network

Upinder Kaur
Assistant Professor, Computer Science, G.M.N College, Ambala Cantt

Abstract - V2X is broadly utilized in the several applications related to the vehicular communication. However, proving security in the V2X network is a big issue. Because of upcoming issues such as dynamic topology, communication latency, network scalability and high processing security algorithms. These issues induce difficulties in proving security to the V2X network. Hence, our main aim and scope is to provide high level security to the V2X network with better data transmission.

I. INTRODUCTION

The upcoming intelligent transport system will rely on the Vehicle to Everything (V2X) communication. The key goal of this V2X communication is to offer road safety and traffic management in the vehicular network [1-2]. The V2X communication is formed as the combination of the Vehicle to Vehicle (V2V) communication, Vehicle to infrastructure (V2I) communication and Vehicle to Pedestrian (V2P) communication. It plays a vital role in the applications such as infotainment, road safety and traffic management. The security providence in V2X network is highly required because of succeeding issues such as entities in vehicular networks are vulnerable to the attacks, false warnings in the network and false data attachment with the transmitted message [3-5]. These issues exemplify the importance of the security in the V2X security.

Authentication is main process in the V2X security which verifies the credentials provided during the time of registration process [6]. The authors in [7] have performed authentication with the aid of the identity based privacy preserving techniques. Here, the batch signature verification process is performed to provide security in V2X. The public key infrastructure (PKI) based authentication process in performed in the V2X where the Elliptic Curve Digital Signature Algorithm is used to generate key for the data transmission [8]. The authors in [9] have contributed elliptic cryptography based authentication in the vehicular network. It pursues authentication by considering the identity based signature procedures.

Routing plays a vital role in the vehicular communication, hence providing security is significant while selecting the forwarder node [10]. To ensure this trust based node selection procedures are emerged in the V2X network. In general, source node considers the two trusts for forwarder node selection [11]. They are direct and indirect trusts. The authors in [12] have utilized two different algorithms for estimation of direct and indirect trusts. In [13] direct trust and recommendation trust is estimated by considering the dropped and forwarded counts of the vehicles. In [14] trust is estimated based on the two factors that are reputation information collection and trust value estimation procedures. A secure and efficient routing protocol (AOMDV) is designed in [15] to provide secure routing in the vehicular network.

1.1 Research Objective

Our main objective is to provide high grade authentication and security in the V2X network to provide secure data transmission. It is achieved through following processes:

- Registration
- Authentication
- Dual Case Routing
- Twofold Verification

II. LITERATURE REVIEW

Reference 1

Title- Multi-array relative positioning for verifying the truthfulness of V2X messages

Concept

In this paper, the trustfulness of the V2X messages is verified using the relative position systems. Here, the physical signals received from the other vehicles are verified with the aid of the multi array relative positioning system. In this, the relative distance between the transmitter and receiver array is considered to verify the trustworthiness of the vehicle to everything network communication messages. Based on the relative positioning information, this paper ensures the V2X transmission messages.

Reference 2

Title- Energy Efficient V2X-Enabled Communications in Cellular Networks

Concept

This paper proposes energy efficient vehicular to everything in the cellular network. Here, the uplink energy consumption is preserved with also ensuring the performance of the delay constraints. This paper provides the V2X communications with the consideration of the delay oriented constraints. Besides, it also allocates the power resource to the vehicle to perform data communication with the other entity in the network. It is obtained with the aid of the quasiconvex optimization algorithm.

Reference 3

Title- Trust Vote: Privacy-Preserving Node Ranking in Vehicular Networks

Concept

This paper proposes the privacy preserving based mechanisms to secure the communication in the vehicular network. Here, the collaborative crowdsourcing-based vehicle reputation system is used which permits vehicles to assess the trustworthiness of other vehicles in the vehicular network. This type of system permits participating vehicles to hide their scores. The proposed procedures also deliberate the trust weight of a vehicle by delivering the rating scores to the vehicles.

Reference 4

Title- Secure Authentication and Key Management with Block chain in VANETs

Concept

This paper introduces the secure authentication and key management in the vehicular network. Here, the block chain is utilized to store the secure credentials of the vehicular network. Here, the certificates less authentication schemes are proposed to secure the data communications in the network. The efficient group keys are utilized to secure the data communications in the network. It also performed dynamic key updation mechanism to reduce the malicious node presence in the network.

Reference 5

Title- A Security Credential Management System for V2X Communications

Concept

In this paper, the security credential management systems are utilized for V2X communication. Here, the public key infrastructure based security management system is considered in the V2X communication system. The pseudonym authority is generating the pseudonym for the particular vehicle in the network. Here, the policy generator is used to update the signature and the keys of the vehicle in the network. Using these procedures, security credentials are managed in the vehicular network.

Problem

- Here, the PKI scheme is utilized to secure the V2X communication which has communication overhead issues

Proposed

- Our approach doesn't utilize the PKI based security schemes which doesn't consumes more communication overhead.

Reference 6

Title- A Mutual Authentication Scheme for Secure Fog Computing Service Handover in Vehicular Network Environment

Concept

This paper proposes the mutual authentication scheme to provide secure communication in vehicular network. Here, the one way hash function and exclusive-or function based operations are utilized to perform authentication in the vehicular network. Furthermore, this paper also provides the secure hand over between the multiple RSU in the vehicular network. In this, the real or random model is performed to analyze the security level of the data transmitted during the transmission.

Reference 7

Title- An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs

Concept

This paper proposes the efficient conditional privacy preserving approach for vehicular network authentication. Here, the identity-based Conditional Privacy-Preserving Authentication (ID-CPPA) signature scheme was introduced to authenticate the nodes in the vehicular network. It pursues the bilinear map based pairing scheme for the authentication. Besides, the identity based signature scheme supports the batch signature verification approach for the authentication purpose.

Problem

- Here, the authentication is performed using the less secure credentials thus introduces malicious nodes participation in the network

Proposed

- We utilize highly secured credentials for the authentication in V2X network thus avoids the malicious node presence in the network.

Reference 8

Title- Fast Confidentiality-Preserving Authentication for Vehicular Ad Hoc Networks

Concept

This paper proposes the confidentiality preserving authentication in the vehicular networks. Initially, it executes the setup phase where the keys are generated using the elliptic curve digital signature algorithm. Using the generated keys vehicles sign their message during data transmission to the destination nodes. The signature generated from the source vehicle is verified in the destination nodes with the aid of the public key provided by the source vehicle. Further, the authentication of the vehicular nodes is performed using the RSU by considering the credentials provided during the registrations.

Problem

- In this, the pre quantum technology is proposed to sign the message during transmission thus doesn't provide high level security such as prevention against quantum computer attack.

Proposed

- In our work, we utilize the post quantum technology based signature generation thus provides high level security in the vehicular network.

Reference 9

Title- An Enhanced Secure Authentication Scheme for Vehicular Ad Hoc Networks without Pairings

Concept

In this paper, the authentication is performed without performing the pairings procedures. Here, the identity based signature verification procedures are pursued to guarantee the secure data communication in the vehicular environment. Here, the elliptic curve algorithm is utilized to sign the transmitted message. By performing signing operation this paper ensures the integrity in the vehicular network. The destination process verifies the signature attached in the data packet transmitted from the source vehicle with the aid of the key transmitted during the data transmission process.

Reference 10

Title- Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network

Concept

This paper proposes the advanced routing mechanism for the vehicular network. Here, the certificate authority is used to authenticate the vehicles in the network. Then key generation is performed using the elliptic curve cryptography algorithm. Here, the secure routing is performed using the enhanced secure AODV protocol. This paper identifies the malicious nodes presence using the threshold value based on the sequence destination number and nonce verification number.

Reference 11

Title- GSTR: Secure multi-hop message dissemination in connected vehicles using social trust model

Concept

In this paper, the secure multi hop message dissemination is performed in the vehicular network. The weight value is assigned to each vehicle by considering its trustworthiness level in the network. Apart from trust value, it also considers the motion of the vehicle in the network in order to select the optimal node to transmit the data packet to the destination. Here, the geographical social trust based routing protocol is utilized to perform data transmission in the vehicular network.

Reference 12

Title- Decentralized Trust Evaluation in Vehicular Internet of Things

Concept

In this paper, the decentralized trust based mechanism is utilized to execute data transmission in the vehicular network. Here, the trust evaluation process considers the two trusts that are direct and indirect. Here, the direct trust is estimated using the fuzzy logic and indirect trust is estimated using the reinforcement algorithm. The direct trust is estimated using the honestness factor, cooperativeness factor and responsibility factor. The indirect trust is estimated using the Q learning algorithm.

Reference 13

Title- A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS).

Concept

In this paper, rouge nodes are detected using the trust estimation in the vehicular network. Here, the rouge node is detected based on the direct and recommendation based trust

estimation procedures. In this, certificate authority provides the unique vehicle identity to the The direct trust is estimated based on the number of dropped packet, number of the forwarded packet and number of packets modified. It accepts the indirect trust from the observer nodes which has high transmission range and smallest distance between the observer node and observed node.

Problem

- Here, the indirect trust provided by the recommenders is not validated using the highly secured mechanisms.

Proposed

- We validate the indirect trust with strong computation mechanism D^2S to avoid malicious node presence in the network.

Reference 14

Title- on Trust Models for Communication Security in Vehicular Ad-hoc Networks

Concept

This paper provides the communication security to the vehicular network using the trust models. Here, the certain factor model is utilized to estimate the trust value for the nodes in the network to perform data transmission. Here, the trust model executes the two stages that are reputation collection and trust value estimation. The direct and indirect reputations are considered for the trust estimation. Based on the estimated reputation, it generates the trust value for the vehicular nodes.

Problem

- Here, the trust estimation is not based on the past behavior of the node thus reduces the security in data transmission

Proposed

- We consider the past behavior of the vehicular node to estimate the trust during data transmission in V2X network.

Reference 15

Title- SE-AOMDV: secure and efficient AOMDV routing protocol for vehicular communications

Concept

In this paper, the secure routing is achieved using the AOMDV routing processes in the vehicular network. Here, the trusted authority authenticates the entities present in the vehicular network. In this paper, the misbehaviors of the nodes are estimated by considering following metrics including sudden change in the vehicle speed, interrupted connections and number of duplicated or dropped packets of the particular vehicle. Based on these factors, it selects the vehicle for routing in the vehicular network.

Reference 16-

Title- A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Networks

Concept

This paper proposes the decentralized lightweight authentication mechanism for V2X network. Here, each vehicle is equipped with Biometric Device (BD) and Tamper Proof Device (TPD). Here, authentication is performed to each vehicle and respective drivers. For authentication, it utilizes the certificate authority (CA) where each driver transmits vehicle real identity, biometric information and information about the vehicle. After receiving these credentials, CA transmits the initial pseudo identity to the respective vehicle TPD. Each driver authenticated using BD, it the biometric is valid. Then, TPD starts processing the signing and verifying the message. In this, hash chain sequence is used to sign the message which is generated by SHA-256 algorithm.

Problem

- Here, the authentication is performed using the BD device which could be easily forgeable and has many technical issues (device default). Since, fake fingerprints are used by malicious users for authentication.
- All the security credentials are stored in the TPD which is not secure since TPD is open source to others. Hence, malicious users can easily identify the security credentials of the drivers.
- The secret key is installed in OBU device during initialization itself which doesn't result in secure V2X communication. Since malicious users can transmit the message using sign generated from this key.
- SHA 256 based sign generation consumes more time thus reduces the processing speed of the signature generation.

Proposed

- Our proposed work performs authentication with the RSU entity. Hence, the security credentials of the users are not forgeable by any malicious users. Besides, we utilize the binary form of the finger vein credentials that increases the security level of data transmission.

- We doesn't provide secret key during initialization process that avoids the malicious users message transmission.
- We utilized bliss digital signature algorithm for integrity verification which performs faster and provides high security.

Reference 17

Title- Secure V2X Communication Network based on Intelligent PKI and Edge Computing

Concept

This paper secures the V2X communication using the intelligent PKI scheme with edge computing technology. Here, keys are distributed by the key distribution center via RSU entity in the network. This paper follows the location based key distribution scheme to secure the V2X communication. Here, the future location of the vehicle is predicted using the Recurrent Neural Network (RNN). For this purpose, RNN utilizes the history routes of the each vehicle. For the estimated future zones, key distribution center distributes keys to the vehicle. By using this key, the vehicle communicates with other vehicles and RSU.

Problem

- Here, PKI based secure V2X communication is performed which tends to increase in the processing or communication overhead due to the large size attached certificate compared to the transmitted message.
- Here, the authentication is not performed using the highly secured credentials such as PUF, Finger Vein and so on. Thus doesn't result in effective authentication procedures in V2X network.
- The keys are transmitted to the vehicle prior based on the future moving zones which doesn't result in secure V2X communication. Since, compromised users can utilize this key to generate signature for their message transmission.

Proposed

- Our work doesn't pursues the PKI based authentication scheme hence we doesn't have communication overhead in the vehicular network.
- In our work we authenticate both users and vehicle using the finger vein, M.S.C, L.No and PUF. Thus provides high security to the V2X data transmission.
- We doesn't provide secret key during initialization process that avoids the malicious users data transmission.

Reference 18

Title- Recommendation-based Trust Model for Vehicle-to-Everything (V2X)

Concept

In this paper, security in the V2X communication is preserved through the recommendation trust model. This paper estimates the trust for each node based on the weighted sum method. Here, the three level trusts are estimated for the secure V2X communication. They are current trust, indirect trust and global trust. The current trust is estimated based on the past trust and direct trust. Here, the confidence level of indirect trust is estimated based on the global trust. Indirect trust is estimated based on the average of the positive and negative recommendations. Here, the confidence level of each recommendation is estimated to remove the false recommendations.

Problem

- Here, the pare to front value estimation based on weight coefficients doesn't provide optimal result in trust estimation. Besides, small change in the weight value leads to drastic effect in the trust estimation. Thus leads to incorrect identification of the malicious node.
- The strong computation mechanisms are required to estimate the confidence level of recommendation trust. Here, the confidence level is estimated again based on the global trust. Thus induces malicious node participation in data transmission in V2X network.

Proposed

- We utilized deng based demspter shafer algorithm for confidence level verification of trust estimated. Thus avoids the malicious node participation in the data transmission. Besides, it identifies the malicious nodes accurately with proper procedures.

Reference 19

Title- An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks

Concept

This paper proposes the secure routing in vehicular network with the aid of the trust estimation. Here, two trusts are estimated to select the optimal forwarder node for routing in the network. They are subjective trust and recommendation trust where the subjective trust is estimated based on the weighted markov prediction algorithm. Here, weighted markov prediction algorithm considers the historical behaviors

of node to evaluate the subjective trust. The evaluation of recommendation trust is accomplished with new recommendation feedback mechanism. The recommendation based feedback mechanism provides creditability to each recommender. Besides, the routing is performed using the light weight trust ware multicast routing protocol (LTMRP).

Problem

- The weighted markov model computes subjective trust using large number of unstructured parameters that tends to increases the difficulties in trust computation.
- The routing is performed through LTMRP protocol which suffers from excessive flooding when increase in the vehicle count. Besides, it also consumes more bandwidth during data transmission.
- Here, the creditability is provided to each recommenders based on the amount of transactions it performed. It is not sufficient to identify the malicious users' presence in the network. Thus introduces more packet losses during data transmission due to presence of malicious nodes.

Proposed

- We perform routing via selecting the optimal forwarder using SHO algorithm which doesn't consumes more bandwidth and flooding during data transmission.
- In our work, we estimate the direct and indirect trust by considering the past behaviors and number of successful transactions. Thus avoids the malicious node participation in the data transmission. Besides, we don't utilize any difficult computation mechanism to estimate the trust value.

Reference 20

Title- CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs

Concept

In this paper, secure data communication is performed using the cooperative pseudonym exchange and scheme permutation mechanism. Initially, it performs the registration process where certificate authority (CA) provides certificate to the each vehicle. The certificate includes the key pair (private and public), long term certificate and base identifier. After registration, using the base identifier vehicle requests the pseudonym to the CA. For cooperative pseudonym exchange, this paper utilizes the two schemes that are random silent period and periodical pseudonym change. It exchanges the pseudonym cooperatively with the neighbor nodes that are in the nearest distance.

Problem

- The cooperative pseudonym exchange scheme doesn't suitable for the sparse vehicular environment. Since it exchanges the pseudonym with more than two neighbors which are in same context.
- Here, credentials considered for the authentication is less confidential due to lack of consideration of high secure credentials for both user and vehicle.
- It also requires regular updation with other vehicles, thus tends to degrade the performances of the network.

Proposed

- In our work, each vehicle itself generates unique pseudo identity for every transmission hence vehicle doesn't need to exchange the pseudo identity with another vehicle.
- In our work, we utilize credentials of both vehicle and user during authentication process in order to provide high level security to the V2X network.
- Besides, our work avoids the frequent updation of pseudo identity with other vehicles thus improves the network performance.

III. PROBLEM STATEMENT

Overall Problem Statement

- In literature, the security in V2X is achieved through the PKI processes. However, PKI based scheme induces more communication overhead and delay in vehicular network.
- None of the works in the V2X have considered high secured credentials (PUF, Finger Vein, and Security Code) for authenticating the vehicles in the network. Thus increases the malicious node presence in the network.
- Most of works utilizes the pre quantum technology to verify its data integrity. However, it suffers from quantum computer attack and low security.
- The trustworthiness of the indirect or recommendation trust is not evaluated effectively with the strong mechanism. It induces more packet losses due to the participation of malicious nodes in the data transmission.

IV. PROPOSED WORK

In our work, we tackle the issues present in the existing V2X security works. Our V2X network comprises of for entities that are *Vehicles, Trusted Authority (TA), RSU and Pedestrians*. Our V2X network supports three communications that are V2V, V2I and V2P. Our main intention is to provide the highly confidential authentication and data security in V2X network. We achieve this intention via implementing the following processes:

4.1. Registration

The primary process in our work is registration where the vehicles register themselves in the TA. In our work, we authenticate both user and vehicles to provide high level security in the V2Xnetwork. For registration, vehicle user transmits four necessary credentials that are *Binary format of user finger vein, Physically Unclonable Function (PUF), Manufacturer Security Code (M.S.C) and License number (L.No).* After receiving vehicle user credentials, TA computes the Pseudo Identity (P.ID) and Keys for the message signing process. Initially, it generates the hash value for L.No and M.S.C using the **Blake2b algorithm**. The hash values of both L.No and M.S.C are processed into the **Quartile Deviation**. The obtained quartile deviation result is considered as P.ID for each vehicle. Besides, the private key (Pr.k) and public keys (Pu.k) to sign the vehicle message are generated using the **Bliss algorithm**. Our proposed bliss algorithm is highly secure compared to other signature generation algorithm. Since, bliss algorithm is post quantum algorithm which provides high level security and fast processing compared to the traditional signature generation algorithm.

4.2. Authentication

In our work, vehicles are authenticated in RSU entity using their credentials. The RSU entity in the network is highly trusted entity and their performance is frequently monitored by the TA for security purpose. Each vehicle authenticates them in the RSU using the credentials including P.ID and First four bits of the binary form of finger vein of user. Here, P.ID is generated by XOR operation of the initial P.ID and Count. It is unique for each transmission in order to provide security in V2X network. Four bits sequence of the finger vein also varied for each transmission sequentially. After receiving the credentials from the users, RSU starts authentication process. It initially checks the credentials provided by the user, if credentials are valid then it grants access to data transmission. For unmatched credentials, it performs following processes: If the unmatched credentials are less than one, then it request L.No and M.S.C credentials to the requested vehicle. If the credentials unmatched are more than one, then it performs PUF challenge-response process. If the credentials are matched, RSU transmits the encrypted form of the Random Number (R.No) and Time Stamp to the source vehicle. Here, the R.No is generated using the **Weierstrass Curve** and encryption is performed using the **Present encryption algorithm**. Further RSU transmits the real R.No and respective key to the destination in order to verify the authorization of the source vehicle.

4.3 Dual Case Routing

In our work, we perform routing with two different cases that are: (i) Pedestrian as Forwarder: If source vehicle want to transmit message to destination, then it checks the presence of the pedestrian in its communication range. If there exist pedestrian then it selects the best pedestrian as a forwarder for the data packet transmission. For this purpose, it estimates the reputation value for each pedestrian. Here, each pedestrian reputation is estimated using their link quality, direction, International Mobile Equipment Identity (IMEI), past successful transmission list (PTL) and Distance. Based on this reputation value, source vehicle selects pedestrian who has highest reputation value. (ii) Vehicle as Forwarder: If there exist no pedestrian in its source communication range, then its go for vehicle based forwarder selection process. In this situation, vehicle performs boundary based forwarder selection scheme. Here, the source vehicle considers the vehicles that are present in its communication boundary. Since, boundary vehicles has less distance to the destination, hence it reduces number of hops. Besides, it also reduces the density of the vehicles considered for the forwarder selection thus fastens the data transmission. For forwarder selection, we use **Deer Hunting Optimization (DHO)** algorithm which considers following parameters such as direct trust, indirect trust, link duration and distance. Here, the direct trust is estimated using the past behaviors and successful transactions. We validate the indirect trust provided by the recommenders using the **Deng based Dempster Shafer (D^2S)** algorithm. Here, the evidence is considered as the distance from the trustee node and successful transmission with the trustee node. By considering these trusts, we select the legitimate forwarder node for routing. Using this algorithm, we remove the trust values provided by the malicious users thus avoids the malicious nodes participation in the data transmission. Before transmitting data packet to the forwarder, it performs the signing process. It is accomplished through the Pr.k provided during the registration process. Using the Pr.k vehicle signs it data packet. Along with generated sign and message, it also attaches the current P.ID generated, Pu.k, E(R.No) and Time Stamp (Ts) to the destination. This way of data transmission provides security to the transmitted data effectually.

4.4. Twofold Verification

Each destination vehicle in the network verifies the data packets transmitted by the source vehicle. It verifies both user authorization and data integrity for the received packet in order to avoid the false information transmission in the network. For the received packet, it initially checks the time stamp and encrypted R.No. It decrypts the R.No attached with the packet using the key provided by the RSU. Then it verifies the decrypted R.No with the transmitted R.No provided by the RSU. If it is same, then it verifies the signature attached with the data packet or else drops the packet. For sign verification process it utilizes Pu.k attached in the data packet received. Using this key, it verifies the signature transmitted by the source. This way of data packet verification provides high

level security in the V2X network. The performance of the proposed work is verified through the upcoming performance metrics,

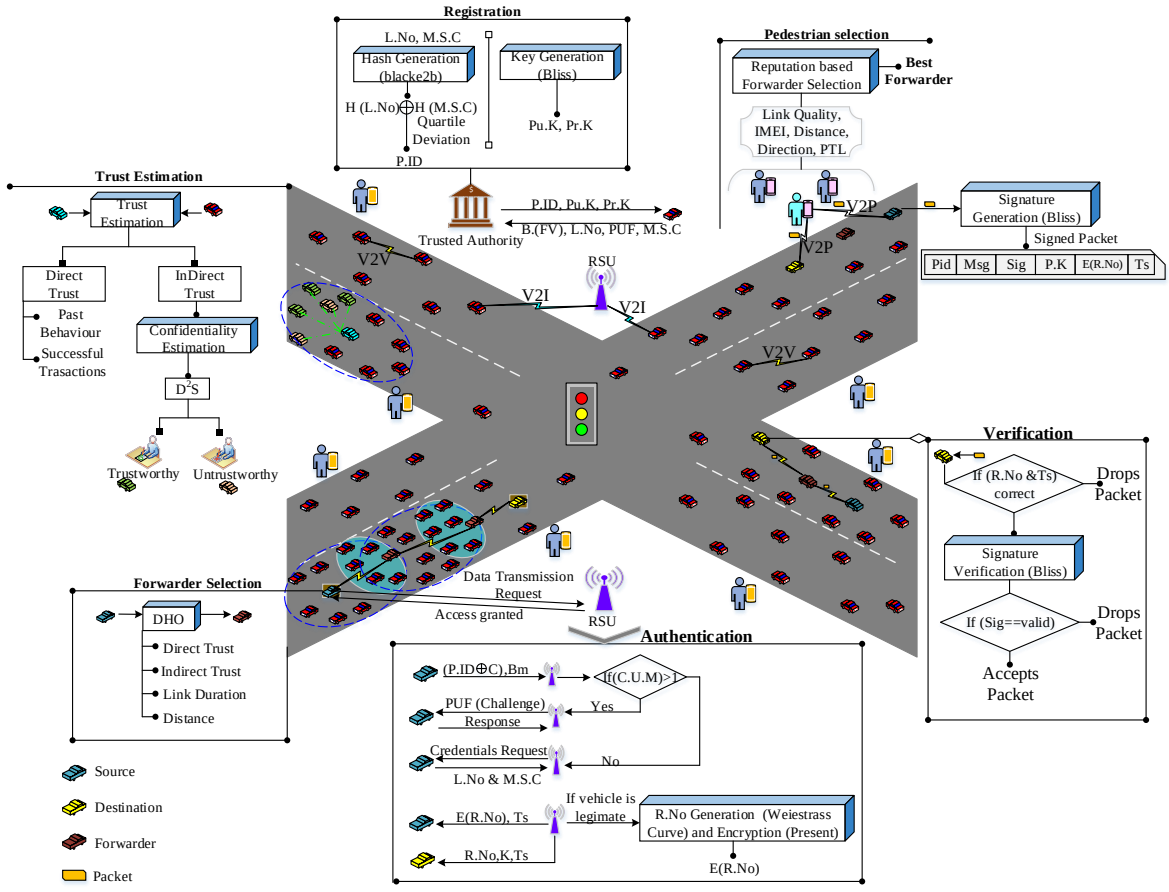
- Packet Delivery Ratio (%)
  - Number of Vehicles
  - Number of malicious nodes
- Throughput (%)
  - Number of Vehicles
  - Number of malicious nodes
- Attack Prediction Rate (%)
- Signature Generation Time (ms)
- End to End delay (ms)

V. RESEARCH HIGHLIGHTS

The highlights of the proposed work are listed as follows:

- Authentication is performed for both user and vehicle using highly secure credentials such as binary form of finger vein, PUF, L.No and M.S.C. Till now, these types of credentials are not utilized for the authentication in the V2X network. Thus differs our work from the preceding V2X security works.
- So far, the received data packets authenticity (source node authorization) is not verified during data transmission. To tackle this issue, our work estimates R.No for each transmission, thus ensures the data packets from the legitimate nodes.
- Our work utilizes the post quantum algorithm namely bliss for signature process. None of the works considers post quantum algorithm based signature verification in the V2X integrity process. It provides high level security and avoids the quantum computer attack in the network.
- We also ensure the indirect trust trustworthiness using the D^2S algorithm. It avoids the malicious nodes participation in the network.
- Our routing is performed using the forwarder selection procedures where we utilized DHO algorithm. It considers the boundary nodes for forwarder selection in order to reduce the forwarder selection time and delay during data transmission in the V2X network.

VI. ARCHITECTURE FOR PROPOSED WORK



VII. REFERENCES

[1] Nguyen, V.-L., Lin, P.-C., & Hwang, R.-H. (2019). Multi-array relative positioning for verifying the truthfulness of V2X messages. IEEE Communications Letters, 1–1.

[2] Zheng, C., Feng, D., Zhang, S., Xia, X.-G., Qian, G., & Li, Y. G. (2018). Energy Efficient V2X-Enabled Communications in Cellular Networks. IEEE Transactions on Vehicular Technology, 1–1.

[3] Azad, M. A., Bag, S., Parkinson, S., & Hao, F. (2018). TrustVote: Privacy-Preserving Node Ranking in Vehicular Networks. IEEE Internet of Things Journal, 1–1.

[4] Tan, H., & Chung, I. (2020). Secure Authentication and Key Management With Blockchain in VANETs. IEEE Access, 8, 2482–2498.

[5] Brecht, B., & Hehn, T. (2018). A Security Credential Management System for V2X Communications. Connected Vehicles, 83–115.

[6] Dewanta, F., & Mambo, M. (2019). A Mutual Authentication Scheme for Secure Fog Computing Service Handover in Vehicular Network Environment. IEEE Access, 7, 103095–103114.

[7] Ali, I., & Li, F. (2019). An efficient conditional privacy-preserving authentication scheme for Vehicle-To-Infrastructure communication in VANETs. Vehicular Communications, 100228.

[8] Mirzaee, S., & Jiang, L. (2019). Fast Confidentiality-Preserving Authentication for Vehicular Ad Hoc Networks. Journal of Shanghai Jiaotong University (Science), 24(1), 31–40.

[9] Jenefa, J., & Mary Anita, E. A. (2019). An Enhanced Secure Authentication Scheme for Vehicular Ad Hoc Networks without Pairings. Wireless Personal Communications.

[10] Tyagi, P., & Dembla, D. (2018). Advanced Secured Routing Algorithm of Vehicular Ad-Hoc Network. Wireless Personal Communications, 102(1), 41–60.

[11] Paranjothi, A., Khan, M. S., Zeadally, S., Pawar, A., & Hicks, D. (2019). GSTR: Secure multi-hop message dissemination in connected vehicles using social trust model. Internet of Things, 7, 100071.

[12] Guleng, S., Wu, C., Chen, X., Wang, X., Yoshinaga, T., & Ji, Y. (2019). Decentralized Trust Evaluation in Vehicular Internet of Things. IEEE Access, 1–1.

[13] Tripathi, K.N., & Sharma, S.C. (2019). A trust based model (TBM) to detect rogue nodes in vehicular ad-hoc networks (VANETS).

[14] Fan, N., & Wu, C. Q. (2019). On Trust Models for Communication Security in Vehicular Ad-hoc Networks. Ad Hoc Networks.

[15] Makhlouf, A.M., & Guizani, M. (2019). SE-AOMDV: secure and efficient AOMDV routing protocol for vehicular communications. International Journal of Information Security, 18, 665-676.

[16] Hakeem, S.A., El-Gawad, M.A., & Kim, H. (2019). A Decentralized Lightweight Authentication and Privacy Protocol for Vehicular Networks. IEEE Access, 7, 119689-119705.

[17] Qiu, H., Qiu, M., & Lu, R. (2019). Secure V2X Communication Network based on Intelligent PKI and Edge Computing. Computer Science

[18] Alnasser, A., Sun, H., & Jiang, J. (2020). Recommendation-Based Trust Model for Vehicle-to-Everything (V2X). IEEE Internet of Things Journal, 7, 440-450.

[19] Xia, H., Zhang, S., Li, Y., Pan, Z., Peng, X.Y., & Cheng, X. (2019). An Attack-Resistant Trust Inference Model for Securing Routing in Vehicular Ad Hoc Networks. IEEE Transactions on Vehicular Technology, 68, 7108-7120.

[20] Singh, P.K., Gowtham, S.N., Tamilselvan, S., & Nandi, S. (2019). CPESP: Cooperative Pseudonym Exchange and Scheme Permutation to preserve location privacy in VANETs. Veh. Commun., 20.