IEEE Access
Multidisciplinary ⁝ Rapid Review ⁝ Open Access Journal

Received 10 July 2023, accepted 24 August 2023, date of publication 4 September 2023, date of current version 11 October 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3311515

RESEARCH ARTICLE

Privacy Aware Post Quantum Secure Ant Colony Optimization Ad Hoc On-Demand Distance Vector Routing in Intent Based Internet of Vehicles for 5G Smart Cities

TANNU SHARMA[1], M. RANJITH KUMAR[2], (Member, IEEE), SACHIN KAUSHAL[1], DHARMINDER CHAUDHARY[3], (Member, IEEE), AND KASHIF SALEEM[4], (Member, IEEE)

[1]Department of Mathematics, School of Chemical Engineering and Physical Science, Lovely Professional University, Phagwara 144001, India
[2]Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Chennai 601103, India
[3]Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai 601103, India
[4]Department of Computer Science and Engineering, College of Applied Studies and Community Service, King Saud University, Riyadh 11362, Saudi Arabia

Corresponding authors: Kashif Saleem (ksaleem@KSU.EDU.SA) and Dharminder Chaudhary (manndharminder999@gmail.com)

This work was supported by the King Saud University, Riyadh, Saudi Arabia, under Researchers Supporting Project number RSPD2023R697.

ABSTRACT The Internet of Vehicles (IoV), with advanced technology in 5G communication, is considered the backbone of a smart city's intelligent transport system. There are mainly two types of vehicular communication: (1) Vehicle to Vehicle (V2V) and (2) Vehicle to Infrastructure (V2I). In IoV, there is a dynamic change in the network topology according to the controllers, destination, vehicle movement, and road structure. Intelligent vehicles are assumed to work with the capacity of data processing, data storage devices, and communication devices to communicate with vehicles or Roadside InfraStructure (RSI). This article presents a post-quantum secure ring learning with error-based key exchange. This assumption ensures security against quantum attacks. The proposed design is an ant colony optimization-based ad hoc ordered distance vector routing algorithm that avoids suspicious vehicles in IoV broadcasting. The proposed framework consists of three parts: (i) certificate authority, (ii) suspicious vehicle detecting algorithm, and (iii) optimal path selection algorithm. The performance analysis section contains an analysis of the proposed design with related ones, and the proposed has better results.

INDEX TERMS Key exchange, optimized routing, the Internet of Vehicles, ring learning with errors, cryptography.

I. INTRODUCTION

Due to a significant technological change, people are integrating it with daily life, making surroundings smart in the form of intelligent automobiles, smart cities, smart homes, smart transportation, etc. The smart transportation system mainly depends on smart automobiles and the Internet of Vehicles (IoV). The IoV is an advanced technology to solve common problems such as traffic congestion, road safety towards accidents, amount of fuel consumption, and air and sound pollution [1], [2]. Smart Transportation systems attracted many sectors, such as governments, academics, and industries, in the form of two types of communication over vehicles: (1) V2V communication and (2) V2I communications [3]. In IoV, data is frequently exchanged between vehicle to vehicle to manage road safety, congestion, and traffic productivity. The optimal connection with other vehicles can be selected instantly using intent-based network design for IoV. For example, an ideal networking route can be determined by (1) the least approximated latency and packet failure rate, (2) maximum speed of data and protection, and (3) minimum routing expenses [4], [5], [6]. The architecture IoV can be utilized in the form of two broad applications: (1) Safety application and (2) Non-safety application. The safety application for IoV includes (a) lane shifting and direction knowledge, (b) announcement of forthcoming traffic and roadway circumstances, and (c) automobile traffic assistance for preventing jams. The non-safety application

The associate editor coordinating the review of this manuscript and approving it for publication was Nurul I. Sarkar.

for IoV includes (a) automatic toll payment, (b) intelligent parking, and (c) access to the web services [3], [7], [8], [9]. A vehicle interacts with another to enjoy internet services, but security and privacy are two major concerns. A general vehicle consists of the individual's identity and a unique number plate. Interaction in IoV usually happens in the following two forms: (1) V2V communication [10], and (2) V2I communication [11]. In IoV communication, any vehicle can be malicious, mainly during vehicle-to-vehicle communication. This type of communication needs both security and privacy. To integrate IoV with security attributes, few research works have been done [12] using cryptography, protection technology, and certificate exchange [13], [14]. But, there are more advanced protocols: (1) anonymous on-demand routing to hide identity and (2) authenticated anonymous, secure routing to establish secure connections. These techniques improve latency and communication overhead for intelligent transportation [15]. But, there are some constraints like effectiveness, security, and privacy in IoV architecture. The current IoV architecture suffers from delay, protection, communication expenses, and lack of privacy preservation. Therefore, we have suggested a framework for IoV based on ring learning with errors and Ant Colony Optimization Ad hoc On-demand Distance Vector (ACO-AODV) routing. The ring learning errors assumption ensures security against quantum attacks, and ACO-AODV improves latency and is used to detect malicious vehicles. The rest of the paper is arranged as the related work is given in Section II. Section III describes the motivation and the contribution of this paper. The reason of utilizing ACO is explained in Section IV. The preliminaries is given in Section V. Section VI describes the proposed privacy aware post-quantum secure ant colony optimization adhoc on-demand distance vector routing protocol. Section VII shows the performance analysis, evaluation, and the discussion. Section VIII concludes the paper.

II. RELATED WORK

This section contains an overview of recent work prior to the proposed framework. Makhlouf and Guizani [16] are the first who introduced the idea of multi-paths distance vectors routing to (1) stop false verification processes, (2) improve automobile disparity, (3) ensure the integrity of transmitted data packets, and (4) monitor network activity to handle routing attacks. Further the increasing demand for perfect privacy, conflicts with a rather more serious security threat called "Sybil Attack" which refers to, the impersonation of one physical entity for many, namely Sybil nodes. In such circumstances, data received from malicious Sybil attackers may seem as if it was received from many distinct physical nodes. Sybil nodes may deliberately mislead other neighbors, resulting in catastrophic situations like traffic jams or even deadly accidents. Hussain and Oh [17] proposed a protocol to protect vehicle communication from Sybil attacks. They aim at two conflicting goals, i.e. privacy and Sybil attack on VANET. In order to avoid Sybil attack through scheduled beacons, they employed a tamper resistant module (TRM) to carry out a pre-assembly data analysis on data that is used to assemble beacons whereas for event reporting message (ERM), and roadside units (RSUs) to localize Sybil nodes in VANET and report them to the revocation authority. Kerrache et al. [18] proposed a method to detect harmful activities of vehicles. The idea was used to unmanned aerial vehicles for detection of malicious activities. Hasrouny et al. [19] proposed a new advanced approach to detect the activity of vehicles. The method is a combination of a hybrid trust model and a misbehavior detection system. The hybrid trust model is used to judge the trust of the vehicle, and it is responsible for reporting malicious activity to the authorities. This is also responsible for deactivating the malicious vehicle. Bylykbashi et al. [20] proposed Fuzzy Clusters Management Systems (FCMSs) for managing vehicular networking systems. The system can be divided into two parts (1) FCMSs1 contains three inputs factors to determine the availability of vehicles in the clusters, and (2) FCMs2 contains parameters identical to those of FCMs1, with the addition of a new parameter vehicle trustworthiness. The results obtained for this system ensure enhanced safety. Wang et al. [21] introduced a lightweight authentication preserving privacy for VANETs. This protocol uses lightweight operation symmetric encryption for authenticating and validating messages. This scheme supports message verification and signing, and reduces message loss ratios and network traffic delays. Zhong et al. [22] introduced a privacy preserving protocol for VANETs supporting conditional privacy. This scheme preserves a vehicle's privacy, and meets the security requirements of authentication, untraceability, and non-repudiation. This protocol allows the trusted authorities to trace malicious vehicles. Li et al. [23] proposed IoV enabling Maritime Transportation Systems (MTS) supporting reliability and low latency, and large scale connectivities. They selected the system parameters to trade-off between reliability and security. Khan et al. [24] proposed an access technique supporting a small-cell IoV network. Gupta et al. [25] proposed a lightweight, load balancing, scalable, and decentralized framework for IoV. This framework opens new research directions where researchers are looking forward to a lightweight blockchain based framework for IoV. Shen et al. [26] proposed a framework supporting both security and efficiency well. The protocol ensures authentication among moving nearby vehicles, edge nodes, and the central cloud. Gupta et al. [27] designed an advanced protocol supporting security functionalities, including unlikability, conditional-traceability, anti-replay, and data authenticity. This protocol is better in terms of energy consumption, data computations, communications, and cryptographic key storage overhead. Zhang et al. [28] introduced a new authentication framework for the IoV to remove overhead over trusted authority. The trusted authority is responsible for generating partial keys using identity, and avoiding key escrow problems. Chen et al. [29] introduced an authentication protocol supporting a better key transfer mechanism to reduce the computations on the cloud. Pan et al. [30] proposed an authentication and key exchange protocol to enable the establishment of a session key between Unmanned Ariel Vehicles and ground station. This protocol uses low cost symmetric encryption technique rather than asymmetric encryption. Both security and efficiency are not easy jobs due to the dynamic behavior of moving vehicles in the IoV. The above discussed protocols improve the security of vehicles in the IoV, but low efficiency causes packet drops, and delay in communication. Therefore, it is highly demanded to design protocol supporting (1) security against quantum attacks and (2) uses optimized routing to detect malicious vehicles.

III. MOTIVATION AND CONTRIBUTION

We have studied [16], [25], [26], [28], [29], [30], [31], [32] and found that these protocols are not secure against quantum attacks. All the protocols [16], [25], [26], [28], [29], [30], [31] Both [16], and [31] don't use optimized routing to detect malicious vehicles. We need to design a protocol that supports (1) security against quantum attacks and (2) uses optimized routing to detect malicious vehicles. The ring learning with errors is an assumption that is efficient and secure against quantum attacks. We have proposed a ring learning with the errors-based protocol that uses Ant Colony Optimization Ad hoc On-demand Distance Vector Routing for the Internet of Vehicles. This also contains an analysis of the proposed and relevant protocols.

IV. WHY ANT COLONY ALGORITHM

In computer science, the ant colony optimization algorithm (ACO) is an optimization probabilistic method to solve computational problems, which is reducible to finding good paths through graphs. The ACO method is very helpful in solving combinatorial optimization problems or routing of vehicles. It is very popular and has been applied to find optimal solutions to the traveling salesman problem (TSP). The major advantage of the ACO method is that it can be run and adapt to changes in realtime. This is the main reason for my interest in network routing and intelligent transportation. Furthermore, in terms of the shortest distance between the vehicles, ACO performs better than GA and SA algorithms. Although both ACO and GA methods are the benchmark to find an optimal solution, ACO is more consistent [33], [34].

V. PRELIMINARIES

The Ring Learning with Errors [35] based key exchange [36] functions in the ring of polynomials $R_p[\omega] = \frac{Z_p[\omega]}{\Phi(\omega)}$ modulo a polynomial $\Phi(\omega) = \omega^n + 1$, beginning with a prime integer modulo (p). Polynomial multiplication and addition would also function as usual, with the results of a multiplication reduced modulo $(\Phi(\omega))$ over the ring. For 256 bits of security, we take $n = 1024$, and prime $p = 40961$, then $\Phi(\omega) = \omega^{1024} + 1$. Ding et al. [36] was the first to suggest the use of "Learning with Errors" and "Ring Learning with Errors" for key exchange, and the security depends upon the solution of well known assumption Learning with Errors over the ring. A typical polynomial is written as follows $b(\omega) = b_0 + b_1.\omega + b_2.\omega^2 + \cdots + b_{n-1}.\omega^{n-1}$, where b_i are the coefficients reduced under modulo (p). If $\Phi(\omega) = \omega^n + 1$ is cylclotomic, then $n = 2^i$ for some $i > 0$ being an integer. The ring learning with errors based key exchange works with polynomials having small infinity norms where it considers the largest coefficient of the polynomial over the set of integers. There are two ways to choose this type of small norm polynomials: (1) uniform sampling from with coefficients from $\{-p, -p+1, \ldots, p-1, p\}$, and Gaussian sampling from $\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$ with mean zero, and standard deviation σ, respectively. Using the ring learning with errors assumption, a user can choose a polynomial $b(\omega)$, and small polynomial $s(\omega)$, and $e(\omega)$ to be kept secret. The user can compute the public key $\varrho(\omega) = b(\omega).s(\omega) + e(\omega)$, and he publishes the public directory through a certificate.

VI. PROPOSED PRIVACY AWARE POST QUANTUM SECURE ANT COLONY OPTIMIZATION AD HOC ON-DEMAND DISTANCE VECTOR ROUTING

A. TECHNOLOGY 5G FOR INTERNET OF VEHICLES

The prevalence and rapid growth of smart terminal network traffic clearly shows the demand for 5G technology and its development. As 5G evolves, both network capacity and spectrum efficiency are constantly improving to give advancement to user experience for different communication techniques and approaches. Recently, the Internet of Vehicles has attracted industry-wide attention for its ability to improve the efficiency of an intelligent vehicular communication system and enhance the user experience. The 5G technology improves Internet of Vehicles communication, and on demand distance vector routing algorithm with an optimization technique that enables to send the valid information directly between vehicles without passing through roadside infrastructures or the network infrastructure. Vehicular communication improves bandwidth efficiency, strengthens communication applications, and improves online experience.

B. CERTIFICATE AUTHORITY AND GENERATING KEYS

To map the vehicle's plate number, we consider a third party, like the Department of Motor Vehicles (DMV) in the United States, as a certification authority (CA) to generate private/public key pairs using ring learning with errors assumption as shown in Fig. 1. The CA is responsible for managing the vehicle plate number, mapping their identity using an encryption key pair, and validating error messages sent by inspecting vehicles and changing the trust value of the vehicle during inspection. The CA creates a certificate for each registered vehicle in a network and also maintains key pairs and vehicle certificates as shown in Fig. 2. An RSU and the DMV would be capable of identifying if the misbehaving vehicle has a valid license number and a certificate, thereby assisting in the protection of users' privacy. In generating keys, ring learning with errors requires less computing power

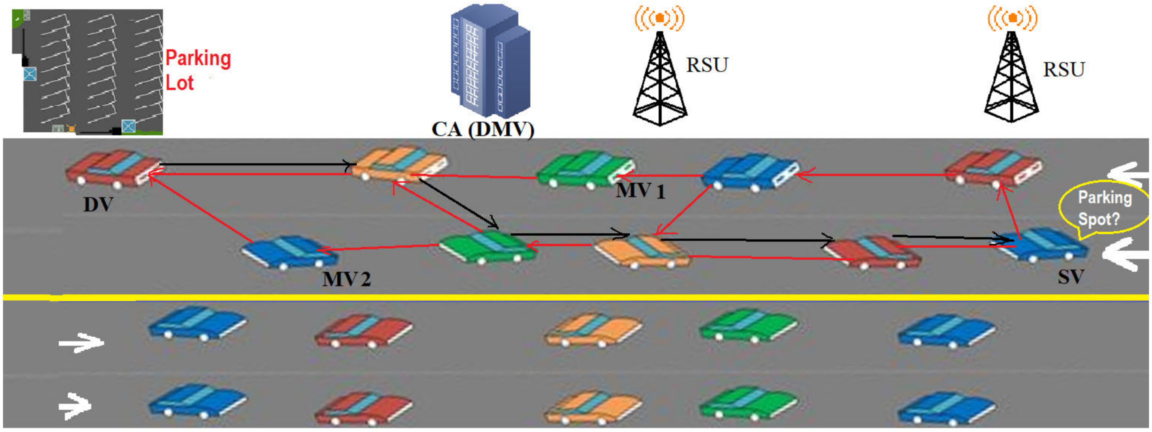

FIGURE 1. CA (DMV) based Proposed Algorithm 1 Scenario to Identify Malicious Vehicles.

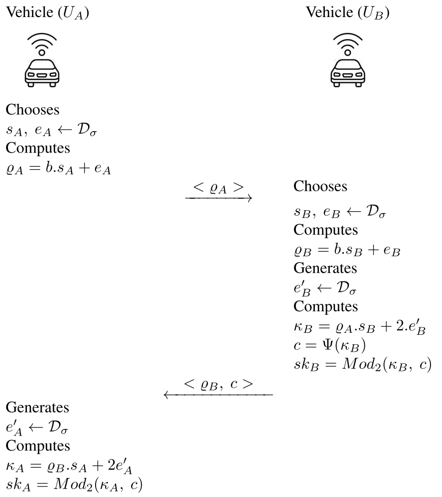
Vehicle (U_A)
Vehicle (U_B)
Chooses
$s_A,\ e_A \leftarrow \mathcal{D}_\sigma$
Computes
$\varrho_A = b.s_A + e_A$
$< \varrho_A >$
Chooses
$s_B,\ e_B \leftarrow \mathcal{D}_\sigma$
Computes
$\varrho_B = b.s_B + e_B$
Generates
$e'_B \leftarrow \mathcal{D}_\sigma$
Computes
$\kappa_B = \varrho_A.s_B + 2.e'_B$
$c = \Psi(\kappa_B)$
$sk_B = Mod_2(\kappa_B,\ c)$
$< \varrho_B,\ c >$
Generates
$e'_A \leftarrow \mathcal{D}_\sigma$
Computes
$\kappa_A = \varrho_B.s_A + 2e'_A$
$sk_A = Mod_2(\kappa_A,\ c)$

FIGURE 2. Key exchange between two vehicles .

and memory compared to other encryption systems, and it is applicable dynamic network of IoV. The vehicle U_A has private key s_A, e_A, and its public key is $\varrho_A = b.s_A + e_A$. Similarly, the vehicle U_B has secret key s_B, e_B, and computes public key $\varrho_B = b.s_B + e_B$, where "b" is public parameter. If an attacker knows ϱ_B, b, then it can't compute s_B, and e_B because ring learning with errors assumption.

The symbol Ψ is signal function defined on $S = \{\lfloor -\frac{p}{4} \rfloor, \ \ldots, \ \lfloor \frac{p}{4} \rceil\} \subseteq \{-\frac{p-1}{2}, \ \ldots, \ \frac{p-1}{2}\}$, where $\lfloor . \rfloor$, and $\lfloor . \rceil$ denotes the floor and rounding to the closest integer. The function $\Psi : Z_p \rightarrow \{0,\ 1\}$ is defined as

$$\Psi(\omega) = \begin{cases} 0, & \omega \in S \\ 1, & \omega \notin S \end{cases}$$

The $Mod_2(.)$ function is defined as $Mod_2(c,\ \omega) = (c + \omega.\frac{p-1}{2})\, mod(p)\, mos(2)$ that is used to eliminate the error term.

C. MALICIOUS VEHICLE DETECTION

Malicious vehicle detection refers to the use of technology and methods to identify vehicles that may pose a threat to public safety. A method for detecting malicious vehicles using frequent communication is proposed in this section. At a particular time (t) $msg_\xi(t)$ is considered to be a legitimate message of a vehicle (ξ) in the Internet of Vehicles. If δ_ξ is added or subtracted in order to change the legitimate message ($msg_\xi \pm \delta_\xi$) then those vehicles are said to be malicious. To enhance the precision of the suggested method, we analyze each vehicle by observing several interactions, which typically consist of exchanging six status messages out of ten that occur within a second. After this careful analysis, we classify a vehicle as nefarious. In the case of N vehicles interacting within a particular road segment during an observation period of $\mathcal{O}_t$, the level of non-confidence of "ξ" is determined.

$$\pi_\xi(t) = \frac{P(\mathcal{O}|T_\xi{=}M)P(T_\xi{=}M)}{\Sigma_{msg=1}^{N} P(\mathcal{O}|T_{msg}{=}M)P(T_{msg}{=}M)}$$

Furthermore, if the instantaneous signal-to-noise ratio (SNR) of a particular signal, denoted as η_ξ, falls below the minimum threshold SNR value $\bar{\eta_\xi}$, then there is a high likelihood of errors occurring in the received messages. Therefore, to address this issue, we factor in the probability of error that arises due to the insufficient instantaneous SNR. This probability of error is calculated as part of the overall analysis

$$P_{\eta_\xi}(t) = Pr\{\eta_\xi < \bar{\eta_\xi}\} = 1 - Pr\{\eta_\xi \geq \bar{\eta_\xi}\}$$

The non-confidence level arises due to a deliberate alteration of a message and the subpar quality of the signal received can be restated as follows.

$$\pi_\xi(t,\ \eta_\xi) = \pi_\xi(t) \times P_{\eta_\xi}(t)$$

Then, the level of confidence of "ξ" can be computed from its level of suspect as

$$\hat{\varphi_\xi} = \hat{\varphi_\xi}(t,\ \eta_\xi) = 1 - \pi_\xi(t,\ \eta_\xi)$$

In our proposed approach for detecting malicious vehicles, we have scrutinized the malevolent activity of the blackhole attack. This type of attack pertains to a situation where a particular vehicle, acting maliciously, exploits the routing protocol by falsely claiming to be the shortest path to the destination vehicle. However, instead of forwarding packets to its neighbors, it drops the routing packets, rendering the communication useless. The occurrence of blackhole attacks is rampant in IoV networks. The trust model we propose is designed to address the issue of vehicles with

Algorithm 1 Detection of Malicious Vehicles and Finding

```
Inputs Periodic status messages from N participating
vehicles and trust threshold level $\lambda_t$, $\xi_m = \emptyset$, $\xi_t = \emptyset$
Repeats
For each vehicle $\xi_i$ do
Computes $\hat{\varphi}\xi_i\xi_i = 1^N$ based on communications
belongs to IoV.
if $\hat{\varphi}_{\xi_i} < \lambda_T$
Vehicle $\xi_i$ is malicious.
$\xi_m = \xi_m \cup \xi_i$
else
Vehicle $\xi_i$ is honest.
$\xi_t = \xi_t \cup \xi_i$
end if
end for
Until exchange of message belongs to IoV
Outputs: non trusty & trusty vehicles: $\xi_m \cap \xi_t = \emptyset$
```

constantly changing behavior, those that transmit incorrect data, and of course, the ones that are malicious. It is important to highlight that while determining the optimal route for data transmission, only reliable vehicles are taken into account. The proposed ACO-AODV algorithm dismisses any malicious vehicles and focuses solely on the trustworthy ones when charting out the data routes.

D. ANT COLONY OPTIMIZED AODVs ROUTING

Adhoc On demand Distance Vectors (AODVs) is a sensitive routing that facilitates route search and recovery in wireless networks. It employs conventional routing tables, which contain a single entry per destination and sequence numbers that verify routing information updates and prevent routing loops. AODV is known for its efficient routing table management and minimal broadcast overhead, as routes are established only when required. ACO-AODV is an enhanced version of AODV that utilizes Ant Colony Optimization (ACO) to identify the optimal path between the source and destination vehicles in the Internet of Vehicles (IoV). The system containing IoV broadcasts messages periodically, and certain applications likewise search a parking spot before the arrival of a vehicle and need more sophisticated routing protocols such as ACO-AODV. The ACO algorithm selects the best route from the possible routes, using request for path, and path-answer methods in conjunction with AODV. The utilization of ACO in AODV enables the protocol to leverage the benefits of both ACO and AODV, resulting in improved routing performance in IoV. ACO leverages the foraging behavior of ants to optimize the path discovery process, while AODV maintains low overhead and efficient routing table management. Algorithm 2 illustrates the ACO algorithm used in ACO-AODV.

The Ant Colony Optimization (ACO) algorithm is an exemplary adaptive method that can effectively transfer information from the previous environment to the next environment and to adapt dynamic change. ACO exhibits remarkable robustness and can handle extreme conditions adeptly. Therefore, ACO traveling salesman is a viable solution for varying routing in the IoVs. The primary objective of the ACO algorithm is to solve the traveling salesman problem efficiently. This problem aims to identify the optimal route that connects more than one vehicle. In the ant system, each ant builds their route and deposits pheromones on the trails it has traveled. The symbol p_{ij}^k denotes the probability of routing request by an ant, k shifting from vehicle's i to vehicle's j. By employing ACO in dynamic routing scenarios, the algorithm can adapt to the frequently changing environment of the Internet of Vehicles. The utilization of ACO in traveling salesman problems can yield a highly optimized route, even in cases where the number of vehicles is vast, and the routes are highly complex.

Algorithm 2 ACO Algorithm

```
Inputs: Possible Paths for Data Communication
Belongs to IoV.
Outputs: Best Path for Data Belongs to IoV
  Repeats
    Repeats
    for Each of Ants/data do
      Chooses new $\xi \in \xi_t$ using state transition
rules and AODVs
      Updates pheromones by (6) and (10).
    end for
  until All paths for routing are investigated.
  All possible data routings are explored.
until Routing is needed.
```

$$p_{ij}^k = \begin{cases} \dfrac{\chi_{ij}^{\alpha} \cdot \gamma_{ij}^{\beta}}{\sum\limits_{l \in \xi_t} \chi_{il}^{\alpha} \cdot \gamma_{il}^{\beta}}, & \text{for } i, j \in \xi_t \\ 0, & \text{otherwise} \end{cases} \tag{1}$$

In the context of ant-based routing protocols, the set of trusted vehicles that an ant or data packet k can visit is represented by ξ_t. The concentrations of pheromone between vehicles i and j, denoted by χ_{ij}, are inversely proportional to delay and distance, while the desirability of transitioning from i to j is indicated by γ_{ij}, where $\alpha \geq 0$ and $\beta (\geq 0)$ determine importance measurement of χ_{ij}, and γ_{ij} respectively. After all the data routes have been built, the pheromone trails are updated. This process involves decreasing the pheromone value to discard previously made poor decisions. The value χ_{ij} computed for two vehicles i and j becomes a part of the process. By considering these parameters, ant-based routing protocols can establish an efficient and optimized route for data transmission between trusted vehicles. The utilization of pheromone trails and their timely updates can help ensure that the most favorable route is chosen, even in complex and dynamic scenarios.

$$\chi_{ij} = \hat{\varphi} j (1 - \rho) \chi_{ij} + \sum_{k=1}^{|Q|} \Delta \chi_{ij}^k, \quad \forall i,\ j \in V_t,\ k \in Q \tag{2}$$

In the proposed routing, the selection of the next hop in a path is determined by the trust level $\hat{\phi}j$ of the neighboring vehicle j, which is calculated based on its previous behavior. This trust level is used to evaluate whether the vehicle j should be included in the set of potential next hops from vehicle i. The pheromone deposition by the kth RREQ/ants for a path from vehicles i to j is denoted by χij^k, and the rate of pheromone evaporation is represented by ρ $(0 \leq \rho \leq 1)$. Additionally, Q is the set of queries/ants in the system.

$$\chi_{ij}^{k} = \begin{cases} \frac{1}{S^k}, & i \in \xi_t \text{ and } j \in \xi_t \text{ uses direct link.} \\ 0, & \text{otherwise.} \end{cases} \tag{3}$$

S^k represents the computation cost associated with the link between ξ_i and ξ_j. The pheromone update method is used by an ant is defined as follows.

$$\chi_{ij} = \hat{\phi}_j(1-\rho)\eta_{ij} + \sum_{k=1}^{|Q|} \Delta\chi_{ij}^{k} + \Delta\eta_{ij}^{best} \tag{4}$$

The pheromone efficiency of ant on the route from ξ_i to ξ_j is $\Delta\chi_{best_{ij}}$.

$$\Delta\chi_{ij}^{best} = \begin{cases} \frac{1}{S}^{best}, & i \in \xi_t \text{ and } j \in \xi_t \text{ uses best link,} \\ 0, & \text{otherwise.} \end{cases} \tag{5}$$

The source SV initiates the process by sending a Route Request (RREQ) to the nearby vehicles (as indicated by the red arrow). Subsequently, each vehicle forwards the RREQ to its closest vehicle, and this continues until it reaches the destination. Notably, Algorithm (1) identifies malicious vehicles such as MV1 and MV2, as depicted in Fig. (1), and these are excluded from consideration for potential data routes.

VII. PERFORMANCE ANALYSIS, EVALUATION AND DISCUSSION

The performance is evaluated on Matlab's simulator over Lenovo, RAM-8GB, Windows 10, Intel i-7 (3.8 GHz). This simulation is carried out by considering four roads with 300 to 600 vehicles with speed following the general normal distribution with a mean of 80 miles and a variance of 60 miles per hour, respectively. This simulation contains nearly 30 percent of malicious vehicles to perform periodical analysis of communicated messages. The proposed design takes the help of the discussed algorithm to analyze honest vehicles, and the optimal path to send data from the source to the destination node. In order to check effectiveness of the proposed routing key exchange denoted [D], we have taken care of other relevant frameworks, [16] denoted [A], [31] denoted [B], and [32] denoted [C] with respect to packet dropping, needed throughput, expected delays, and overhead by routing in the IoV. The analysis is mainly performed with several components like average delay, communication bits, single vehicle throughput, dropping rate of packets, and overhead by routing. The dropping rate of packets denotes the ratio of the packets received at the receiver end to those sent from the source within specific time periods. The Fig. (3) shows the expected rate of packet dropping versus the number of nodes in the IoV. The expected drop rate of packets analyses how many of them were transmitted and received successfully within a period. The Fig. (3) shows more vehicles in an IoV causes more drop rate. It concludes nodes in the IoV are directly connected to the packet drop rate. The Fig. (3) also shows the proposed design ensures less packet loss rate, the highest trust and the least congestion. The Fig. (4) represents the expected throughput, and it also analyses the mean of periods to sent messages from the source to the target. The expected delay shows an increment directly to the number of nodes in the IoV. However, the proposed design takes low expected delay whenever we consider trusted IoV. The Fig. (5) contains analysis of expected throughput for the proposed and the relevant frameworks [16], [31], and [32].

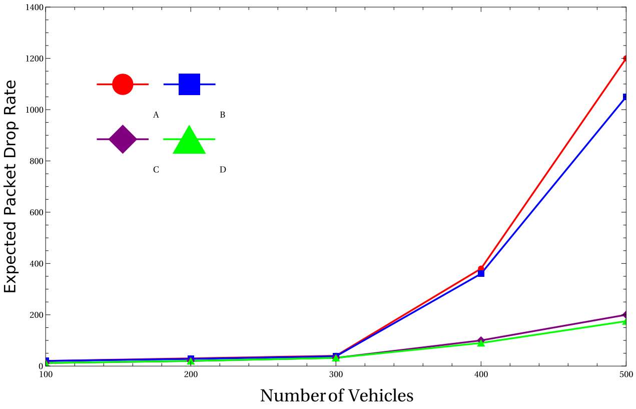

FIGURE 3. Packet drop rate comparison among related frameworks.

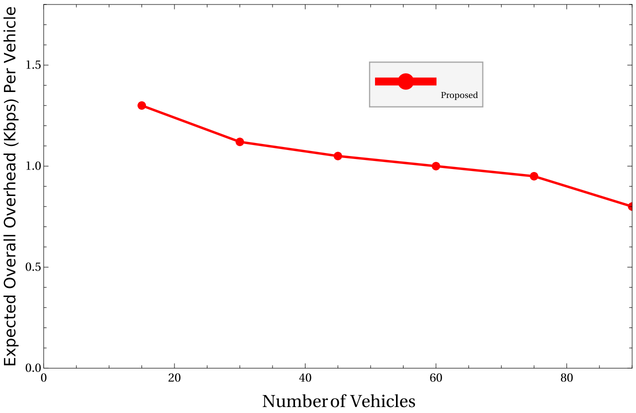

FIGURE 4. Expected throughput vs the percentage of malicious nodes variations.

The Fig. (5) contains an analysis to prove the proposed routing framework has a better performance than [16], [31], and [32]. Moreover, the Fig. (6) contains the analysis of the vehicle's expected throughput versus average speed, and the proposed framework has better performance than [16], [31], and [32]. The Fig. (7) shows expected overhead during routing versus the number of vehicles. The overhead varies

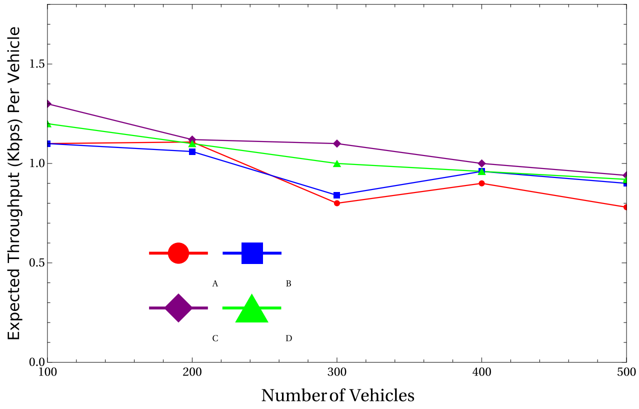

FIGURE 5. Expected throughput comparison among related frameworks.

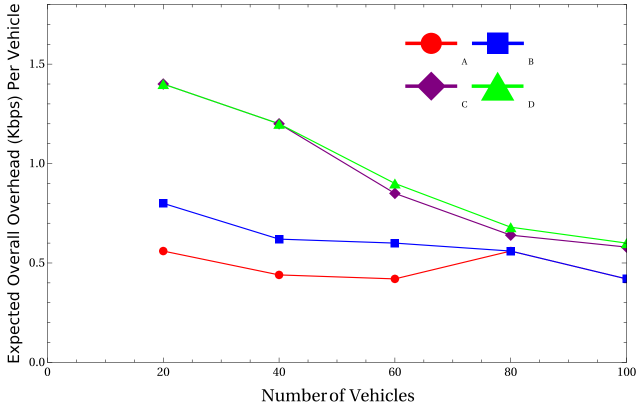

FIGURE 6. Expected throughput versus average speed comparison.

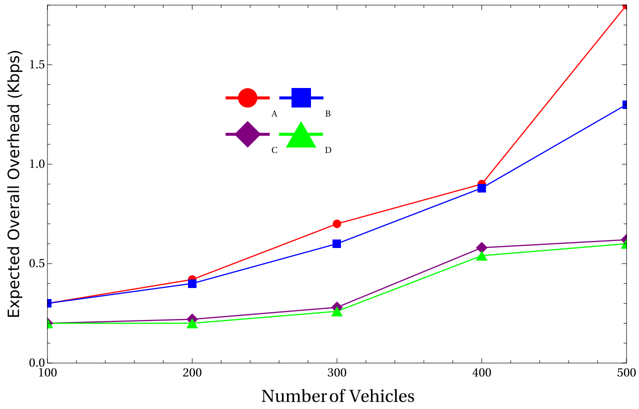

FIGURE 7. Transaction latency comparison among related frameworks.

with the number of needed packets to be routed. The proposed framework has low overheads because it uses a detection algorithm for doubtful vehicle. The Fig. (8) shows the expected drop rate of packets versus the percentage of doubtful vehicles, and it records an increment in the dropping rate, and it reaches to worst level at the value 158 with the percentage of malicious nodes at 87 percent.

VIII. CONCLUSION

The proposed design uses ring learning with errors assumption that makes it secure against quantum attacks. The Internet of Vehicles enables more than one vehicle to transfer confidential information using an on-demand distance vector

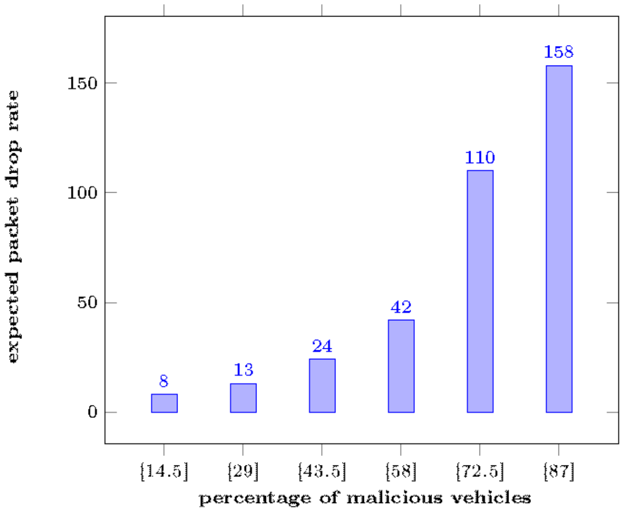

FIGURE 8. Analysis of expected drop rate of packets with respect to malicious vehicle percentage.

routing assisted networking system. The proposed protocol can handle IoV with dynamic change in network-topology according to the controllers, destination, destination or vehicle movement and road structure. This framework ensures both security and latency, and it uses an optimized path algorithm based on ad hoc ordered distance vector routing. It also uses an advanced detection algorithm that prevents suspicious vehicles from entering in the communication framework of IoV. The performance analysis ensures that the proposed framework is more suitable than existing ones.

ACKNOWLEDGMENT

The authors would like to thank the "Researchers Supporting Project number (RSPD2023R697), King Saud University, Riyadh, Saudi Arabia" for supporting the work.

REFERENCES

[1] N. Kumar, S. Misra, J. J. P. C. Rodrigues, and M. S. Obaidat, "Coalition games for spatio-temporal big data in Internet of Vehicles environment: A comparative analysis," *IEEE Internet Things J.*, vol. 2, no. 4, pp. 310–320, Aug. 2015.

[2] M. Gerla, E.-K. Lee, G. Pau, and U. Lee, "Internet of Vehicles: From intelligent grid to autonomous cars and vehicular clouds," in *Proc. IEEE World Forum Internet Things (WF-IoT)*, Mar. 2014, pp. 241–246.

[3] D. B. Rawat and C. Bajracharya, "Adaptive connectivity for vehicular cyber-physical systems," in *Vehicular Cyber Physical Systems: Adaptive Connectivity and Security*. New York, NY, USA: Springer, 2017, pp. 15–24.

[4] K. Saleem, A. Derhab, M. A. Orgun, and J. Al-Muhtadi, "Analysis of the scalability and stability of an ACO based routing protocol for wireless sensor networks," in *Proc. 12th Int. Conf. Inf. Technol.—New Gener.* IEEE, Apr. 2015.

[5] K. Saleem, N. Fisal, and J. Al-Muhtadi, "Empirical studies of bio-inspired self-organized secure autonomous routing protocol," *IEEE Sensors J.*, vol. 14, pp. 2232–2239, Jul. 2014.

[6] K. Saleem and I. Ahmad, "Ant colony optimization ACO based autonomous secure routing protocol for mobile surveillance systems," *Drones*, vol. 6, p. 351, Nov. 2022.

[7] S. S. Manvi and S. Tangade, "A survey on authentication schemes in VANETs for secured communication," *Veh. Commun.*, vol. 9, pp. 19–30, Jul. 2017.

[8] P. Golle, D. Greene, and J. Staddon, "Detecting and correcting malicious data in VANETs," in *Proc. 1st ACM Int. Workshop Vehicular Ad Hoc Netw.*, 2004, pp. 29–37.

[9] J. A. Chaudhry, K. Saleem, M. Alazab, H. M. A. Zeeshan, J. Al-Muhtadi, and J. J. P. C. Rodrigues, "Data security through zero-knowledge proof and statistical fingerprinting in vehicle-to-healthcare everything (V2HX) communications," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, pp. 3869–3879, Jun. 2021.

[10] X. Yang, J. Liu, F. Zhao, and N. H. Vaidya, "A vehicle-to-vehicle communication protocol for cooperative collision warning," in *Proc. 1st Annu. Int. Conf. Mobile Ubiquitous Syst., Netw. Services (MOBIQUITOUS)*, 2004, pp. 114–123.

[11] C.-H. Ou, "A roadside unit-based localization scheme for vehicular ad hoc networks," *Int. J. Commun. Syst.*, vol. 27, no. 1, pp. 135–150, Jan. 2014.

[12] V. Hoa La and A. Cavalli, "Security attacks and solutions in vehicular ad hoc networks: A survey," *Int. J. AdHoc Netw. Syst.*, vol. 4, no. 2, pp. 1–20, Apr. 2014.

[13] S. Jiang, X. Zhu, and L. Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," *IEEE Trans. Intell. Transp. Syst.*, vol. 17, no. 8, pp. 2193–2204, Aug. 2016.

[14] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, and J. Zhou, "A new payment system for enhancing location privacy of electric vehicles," *IEEE Trans. Veh. Technol.*, vol. 63, no. 1, pp. 3–18, Jan. 2014.

[15] W. Liu and M. Yu, "AASR: Authenticated anonymous secure routing for MANETs in adversarial environments," *IEEE Trans. Veh. Technol.*, vol. 63, no. 9, pp. 4585–4593, Nov. 2014.

[16] A. M. Makhlouf and M. Guizani, "SE-AOMDV: Secure and efficient AOMDV routing protocol for vehicular communications," *Int. J. Inf. Secur.*, vol. 18, no. 5, pp. 665–676, Oct. 2019.

[17] R. Hussain and H. Oh, "On secure and privacy-aware Sybil attack detection in vehicular communications," *Wireless Pers. Commun.*, vol. 77, no. 4, pp. 2649–2673, Aug. 2014.

[18] C. A. Kerrache, A. Lakas, N. Lagraa, and E. Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," *Veh. Commun.*, vol. 11, pp. 1–11, Jan. 2018.

[19] H. Hasrouny, A. E. Samhat, C. Bassil, and A. Laouiti, "Trust model for secure group leader-based communications in VANET," *Wireless Netw.*, vol. 25, no. 8, pp. 4639–4661, Nov. 2019.

[20] K. Bylykbashi, D. Elmazi, K. Matsuo, M. Ikeda, and L. Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," *Cognit. Syst. Res.*, vol. 55, pp. 153–163, Jun. 2019.

[21] M. Wang, D. Liu, L. Zhu, Y. Xu, and F. Wang, "LESPP: Lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," *Computing*, vol. 98, no. 7, pp. 685–708, Jul. 2016.

[22] H. Zhong, J. Wen, J. Cui, and S. Zhang, "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET," *Tsinghua Sci. Technol.*, vol. 21, no. 6, pp. 620–629, Dec. 2016.

[23] X. Li, Y. Zheng, M. D. Alshehri, L. Hai, V. Balasubramanian, M. Zeng, and G. Nie, "Cognitive AmBC-NOMA IoV-MTS networks with IQI: Reliability and security analysis," *IEEE Trans. Intell. Transp. Syst.*, vol. 24, no. 2, pp. 2596–2607, Feb. 2023.

[24] W. U. Khan, X. Li, A. Ihsan, M. A. Khan, V. G. Menon, and M. Ahmed, "NOMA-enabled optimization framework for next-generation small-cell IoV networks under imperfect SIC decoding," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 11, pp. 22442–22451, Nov. 2022.

[25] M. Gupta, R. B. Patel, S. Jain, H. Garg, and B. Sharma, "Lightweight branched blockchain security framework for Internet of Vehicles," *Trans. Emerg. Telecommun. Technol.*, p. e4520, 2022, doi: 10.1002/ett.4520.

[26] M. Shen, H. Lu, F. Wang, H. Liu, and L. Zhu, "Secure and efficient blockchain-assisted authentication for edge-integrated Internet-of-Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 11, pp. 12250–12263, Nov. 2022.

[27] D. S. Gupta, A. Karati, W. Saad, and D. B. da Costa, "Quantum-defended blockchain-assisted data authentication protocol for Internet of Vehicles," *IEEE Trans. Veh. Technol.*, vol. 71, no. 3, pp. 3255–3266, Mar. 2022.

[28] H. Zhang, Y. Lai, and Y. Chen, "Authentication methods for Internet of Vehicles based on trusted connection architecture," *Simul. Model. Pract. Theory*, vol. 122, Jan. 2023, Art. no. 102681.

[29] C.-M. Chen, Z. Li, S. Kumari, G. Srivastava, K. Lakshmanna, and T. R. Gadekallu, "A provably secure key transfer protocol for the fog-enabled social Internet of Vehicles based on a confidential computing environment," *Veh. Commun.*, vol. 39, Feb. 2023, Art. no. 100567.

[30] X. Pan, Y. Jin, and F. Li, "An efficient heterogeneous authenticated key agreement scheme for unmanned aerial vehicles," *J. Syst. Archit.*, vol. 136, Mar. 2023, Art. no. 102821.

[31] P. Tyagi and D. Dembla, "Performance analysis and implementation of proposed mechanism for detection and prevention of security attacks in routing protocols of vehicular ad-hoc network (VANET)," *Egyptian Informat. J.*, vol. 18, no. 2, pp. 133–139, Jul. 2017.

[32] S. Safavat and D. B. Rawat, "On the elliptic curve cryptography for privacy-aware secure ACO-AODV routing in intent-based Internet of Vehicles for smart cities," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 8, pp. 5050–5059, Aug. 2021.

[33] H. M. El Din, "Comparative analysis of ant colony optimization and genetic algorithm in solving the traveling salesman problem," vol. 2013, 2021, Art. no. 123738.

[34] H. H. A. Mukhairez and A. Y. A. Maghari, "Performance comparison of simulated annealing, GA and ACO applied to TSP," *Int. J. Intell. Comput. Res.*, vol. 6, no. 4, pp. 647–654, Dec. 2015.

[35] V. Lyubashevsky, C. Peikert, and O. Regev, "On ideal lattices and learning with errors over rings," *J. ACM*, vol. 60, no. 6, pp. 1–35, Nov. 2013.

[36] J. Ding, X. Xie, and X. Lin, "A simple provably secure key exchange scheme based on the learning with errors problem," *IACR Cryptol. ePrint Arch.*, vol. 2012, 2012. [Online]. Available: https://api.semanticscholar.org/CorpusID:583933

TANNU SHARMA received the B.Sc. and M.Sc. degrees in mathematics from Kurukshetra University. She is currently pursuing the Ph.D. degree in security and privacy of the Internet of Vehicles with Lovely Professional University, Jalandhar, India. Her current research interests include cryptography, vehicular communication, and security and privacy in the IoV and the IoT.

M. RANJITH KUMAR (Member, IEEE) received the Ph.D. degree in cryptography and network security. He is currently an Assistant Professor (Selection Grade) with the Department of Mathematics, Amrita School of Engineering, Amrita Vishwa Vidyapeetham, Chennai, India. He has published 20 SCI/Scopus-indexed articles in the areas of cryptography and network security and the Internet of Drones/Vehicles security.

SACHIN KAUSHAL received the B.Sc. and M.Sc. degrees in mathematics from Kurukshetra University. He is currently an Assistant Professor with Lovely Professional University, Jalandhar, India. His current research interests include cryptography, vehicular communication, and security and privacy in the IoV and the IoT.

DHARMINDER CHAUDHARY (Member, IEEE) received the Ph.D. degree in cryptography and network security. He is currently an Assistant Professor (Senior Grade) with the Department of Computer Science and Engineering, Amrita School of Computing, Amrita Vishwa Vidyapeetham, Chennai, India. He has published 30 SCI/Scopus-indexed articles in the areas of cryptography and network security and the Internet of Drones/Vehicles security.

KASHIF SALEEM (Member, IEEE) received the B.Sc. degree in computer science from Allama Iqbal Open University, Islamabad, Pakistan, in 2002, the PGD degree in computer technology and communication from Government College University, Lahore, Pakistan, in 2004, and the M.E. degree in electrical engineering electronics and telecommunication and the Ph.D. degree in electrical engineering from the University of Technology Malaysia, in 2007 and 2011, respectively. Since 2012, he has been with the Center of Excellence in Information Assurance (CoEIA), King Saud University, Saudi Arabia, where he is currently an Associate Professor. He is also an Adjunct Professor with the Department of Computer Sciences and Engineering, College of Applied Studies and Community Service, King Saud University. He is professionally certified by the Massachusetts Institute of Technology (MIT) in cybersecurity, the University of the Aegean in information and communication security, Institut Mines-Télécom in queuing theory, IBM in security intelligence analyst, and Microsoft and Cisco in computer networks. He acquired several research grants in Saudi Arabia, EU, and other parts of the world. He has authored or co-authored over 140 papers in refereed journals and international conferences. His research interests include ubiquitous computing, mobile computing, the Internet of Things (IoT), machine-to-machine (M2M) communication, wireless mesh networks (WMNs), wireless sensor networks (WSNs), and mobile adhoc networks (MANETs), intelligent autonomous systems, information security, and bioinformatics. He served as a technical program committee member and organized numerous international workshops and conferences. He is providing services as an Associate Editor mainly to *Alexandria Engineering Journal*, *Journal of Multimedia Information System* (JMIS), IEEE Access, *International Journal of E-Health and Medical Communications* (IJEHMC), and *International Journal of Cyber-Security and Digital Forensics* (IJCSDF).