On the Elliptic Curve Cryptography for Privacy-Aware Secure ACO-AODV Routing in Intent-Based Internet of Vehicles for Smart Cities

Sunitha Safavat and Danda B. Rawat, *Senior Member, IEEE*

***Abstract*—Internet of Vehicles (IoV) in 5G is regarded as a backbone for intelligent transportation system in smart city, where vehicles are expected to communicate with drivers, with road-side wireless infrastructure, with other vehicles, with traffic signals and different city infrastructure using vehicle-to-vehicle (V2V) and/or vehicle-to-infrastructure (V2I) communications. In IoV, the network topology changes based on drivers' destination, intent or vehicles' movements and road structure on which the vehicles travel. In IoV, vehicles are assumed to be equipped with computing devices to process data, storage devices to store data and communication devices to communicate with other vehicles or with roadside infrastructure (RSI). It is vital to authenticate data in IoV to make sure that legitimate data is being propagated in IoV. Thus, security stands as a vital factor in IoV. The existing literature contains some limitations for robust security in IoV such as high delay introduced by security algorithms, security without privacy, unreliable security and reduced overall communication efficiency. To address these issues, this paper proposes the Elliptic Curve Cryptography (ECC) based Ant Colony Optimization Ad hoc On-demand Distance Vector (ACO-AODV) routing protocol which avoids suspicious vehicles during message dissemination in IoV. Specifically, our proposed protocol comprises three components: i) certificate authority (CA) which maps vehicle's publicly available info such as number plates with cryptographic keys using ECC; ii) malicious vehicle (MV) detection algorithm which works based on trust level calculated using status message interactions; and iii) secure optimal path selection in an adaptive manner based on the intent of communications using ACO-AODV that avoids malicious vehicles. Experimental results illustrate that the proposed approach provides better results than the existing approaches.**

***Index Terms*—Elliptic Curve Cryptography (ECC), Ad hoc On-Demand Distance Vector (AODV), Ant Colony Optimization (ACO) and ACO-AODV (ACO-AODV).**

I. Introduction

Lately, smart transportation system has become one of the important components of human life. Smart cities are relying on different applications such as smart transportation system, smart energy grid, smart healthcare, smart water systems and so on. Smart transportation system is expected to rely heavily on smart vehicles and Internet of Vehicles (IoV) along with 5G and Beyond. IoV in smart transportation system is emerging to solve challenges associated with traffic safety, traffic congestion, fuel consumption and road accidents along with pollution [5], [13]. In the past decades, smart transportation system was emerged with attention to industries, governments and academia by introducing communications among vehicles using vehicle-to-vehicle communications or vehicle-to-roadside communications forming IoV [6], [26]. The vision for IoV encompasses the recurrent exchange of data by vehicles to ease route planning, road safety, traffic efficiency and infotainment applications. Intent-based networking for IoV helps to choose the best networking parameters on the fly (like in software-defined networking) such as the best routing path based on i) lowest estimated delay and packet drop rate, ii) highest data rate and security (with trustworthy vehicles) and iii) lowest routing overhead, where decision making parameters are learned on the fly or predicted based on the history.

Different applications of IoV can be broadly classified as i) safety applications and ii) non-safety applications. The safety applications include: a) vehicle collision and congestion avoidance, b) notification of upcoming traffic and road conditions, c) vehicles lane change and navigation information and d) vehicles traffic support such as traffic flow along with traffic conditions for averting traffic jams. The non-safety applications include: a) electronic toll collection, b) smart parking system, c) entertainment, and (d) Internet access [7]. Secure communication and reliable information in IoV are important for each of these applications [8], [26]. Furthermore, vehicles are owned for long time and are regarded as private properties. Vehicles identities are connected to drivers/owners. Thus, privacy and security are equally important in IoV. Typically, communication in IoV occurs as : 1) vehicle to vehicle (V2V) communications [9] and 2) vehicle to roadside (V2R) communications with possible inter-roadside communications [10]. These communications help to disseminate the traffic information in IoV in a timely manner. However, there are numerous attacks to mislead the vehicles or communications in IoV. Such attacks include worm-hole, black hole and false data injection in addition to Sybil attack [6], [26]. In IoV, any vehicles could be malicious when V2V communication is used and more attacks are possible in IoV with V2V communications. Thus, when V2V communications are used, security and privacy stand as vital factors in IoV. To provide secure communications in IoV, there have been quite a few research works [11],

Manuscript received Day Month Year.

Authors are with the Data Science & Cybersecurity Center (DSC^2), Department of Electrical Engineering and Computer Science at Howard University, Washington, DC 20059, USA. Corresponding E-mail: db.rawat@ieee.org, danda.rawat@howard.edu.

This work was supported in part by the US NSF under grants CNS 1650831 and HRD 1828811, and by the U.S. Department of Homeland Security under grant DHS 2017-ST-062-000003 and by the DoE's National Nuclear Security Administration (NNSA) Award # DE-NA0003946. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

[26]. There have been different approaches including use of cryptographic, security engineering, and certificate exchange methods [12], [15], Anonymous on-demand routing (ANODR) to hide the identity, AASR (authenticated anonymous secure routing) based on cryptographic and public key infrastructure for instituting secure network connection and so on. These approaches introduce extra routing overhead in terms of delay and communication overhead [16].

However, existing literature contains limitations for robust security and privacy in IoV in terms of high delay introduced by security algorithms, unreliable IoV security, high communication overhead and no privacy aware security. To address these issues while providing better security with privacy, we propose a secure communications in IoV (in the presence of malicious vehicles) using modified Elliptic Curve Cryptography (ECC) and Ant Colony Optimization Ad hoc On-demand Distance Vector (ACO-AODV) routing protocol.

Proposed approach comprises three components for IoV: i) certificate authority (CA) which maps vehicle's publicly available info such as number plates with cartographic keys using ECC; ii) malicious vehicle (MV) detection algorithm which works based on trust level of vehicles which is calculated using periodic status message interactions; and iii) secure Optimal Path (OP) selection in an adaptive manner based on the intent of communications using ACO-AODV that avoids malicious vehicles. We present an analysis and simulation results that support our claims. Furthermore, numerical results obtained from simulations show that the proposed approach gives better performance (in terms of throughput, delay, packet drop rate, etc.) than the existing approaches.

The rest of the paper is organized as follows. Section II briefly reviews the related works. In Section III, system model is presented. Section IV presents proposed approach followed by the Section V with simulation results and discussion for performance evaluation. Finally, Section VI concludes the paper.

II. Literature Review

This section presents a brief review on the recent research works related to our proposed approach and the problem considered in the paper.

Amel Makhlouf et. al. proposed a Secure and Efficient-Ad hoc On-demand Multi-path Distance Vector (SE-AOMDV) routing protocol [17] to 1) abandon fake vehicles utilized by the authentication processes, 2) strengthen vehicle disjuncture, 3) assure the delivered packet integrity and 4) observe the network behavior to detect routing attacks.

Rasheed Hussain and Heekuck Oh [18] proposed an approach for securing vehicular communications against Sybil attack and privacy concerns. The Sybil attack was launched via scheduled beacons and Event Reporting Messages (ERM), and hence recommended a Sybil attack prevention or detection framework for the ERM and scheduled beacons. For scheduled beacons, this framework employed TRM (Tamper Resistant Module) to execute a pre-assembly analysis on the data received as of outer modules for assembling beacons. But for ERM, RSI issue authenticated tokens to the vehicles whilst reporting ERMs. This framework preserved user privacy in case of both ERM and beacons by omitting the recognized information as of aforementioned messages and yet revocable if required.

Chaker Kerrache et al. [20] recommended a solution for detecting the intelligent malicious vehicle behaviors based on the adaptive detection threshold. The proposed approach utilized a new Unmanned Aerial Vehicles (UAV)-assisted trust centric scheme based on threshold adaptive control method to discard attackers. The proposed approach also incited attackers to act well when any malicious behavior was detected.

Hamssa Hasrouny et al. [21] proffered a secure framework centered on the vehicle's behavior analysis. The approach has an HTM (Hybrid Trust Model) and MDS (Misbehavior Detection System) where a trust metric was allotted to every vehicle contingent on its behavior. In this approach, HTM judges the vehicle's trustworthiness and reports an MA (Misbehavior Authority) and takes appropriate actions and deactivates the malicious vehicle. Results evinced that the model selected trustworthy vehicles and monitored their behaviors and classified them and deactivated the malicious vehicle.

Kevin Bylykbashi et al. [22] proffered a Fuzzy Cluster Management System (FCMS) for the vehicular network. The system comprised 2 fuzzy-centric systems. i) FCMS1 regarded 3 linguistic input parameters: VRSVC (Vehicle Relative-Speed with Vehicle Clusters), VDC (Vehicle Degrees of Centrality) and VS (Vehicle Security) decided the VRLC (Vehicle Remain or Leave Clusters) possibility output parameter. ii) FCMS2 regarded 4 parameters: 3 parameters were same as FCMS1 parameters and a new parameter was added, which was termed VT (Vehicle Trustworthiness). The outcomes evinced that this scheme proffered better security.

Mingzhong Wang et al. [24] proposed a scheme termed LESPP (Light-weight and Efficient Authentication with the strong Privacy Preservation) for the secured VANET communication. This scheme was chiefly deployed symmetric operations for message sign and verification, which diminished both communication and computational overhead. The identification centered signature utilized by KMC (Key Management Center) to sign messages that do not need to transmit a certificate together with the message, which further diminished communication overhead and averted the certificate management. Extensive simulation exhibited that the scheme was feasible and shown a pre-eminent performance regarding network delay, message verification/signing, and message-loss ratio.

Zhong et al. [25] suggested conditionals privacy-preserving authentications intended for VANETs that considers the security of communication messages, vehicle user's privacy, and the computational power of vehicle nodes. The security scrutiny showed that the suggested scheme not merely satisfies the security acquirement like message authentication, unlinkability, non-repudiation, and replay resistance but also preserved the vehicles' privacy while ensuring the Trusted Authority could track them. The performance assessment indicated that the scheme was more effective than the existent schemes regarding computation cost and communication overhead, which makes it more apt for deployment in IoV services in addition to applications.

Huang et.al. [31] proposed Blockchain System with Credit-Based Consensus Mechanism for establishing a desirable trust model in VANETs. The underlying technology of the Bitcoin protocol is a distributed public ledger encrypted using Merkel trees and hash functions and has a consensus mechanism based on a proof of work (PoW) algorithm. These significant features of blockchain make it potential for establishing a desirable trust model in VANETs. All the broadcasted messages and activities of authorities will be written into the immutable and unforgeable ledger, which can be verified and audited by every entity in the network. However, the privacy of nodes was not considered at the time of Bitcoin's original design. By reviewing the ledger, the transactions made with any public key is traceable to a real identity.

Due to the dynamic network architecture, the IoV networks cannot be secured by the existing security solutions [2], [27]. Therefore, researchers have proposed different approaches to enhance security. Li et al. [28] also introduced the trust establishment scheme in VANETs to help normal nodes make the right choice and constrain the harmful behavior of bad ones. N Bißmeyer et al. [29] proposed that trustworthy communication in vehicular ad hoc networks is essential to provide a reliable traffic safety to improve the efficiency of applications. Moreover, the author in [30] refer to trust and reputation management in distributed networks as a novel and original way to address and tackle some of those not yet solved threats. However, the existing solutions could not solve the security and privacy issues in IoV instead increased network overhead and reduced system efficiency. Hence, more research work on trust management has to be done.

All of these approaches provide some level of enhanced security while avoiding malicious vehicles but introduce high overhead in terms high delay, unreliable security without considering privacy of the drivers, reduced throughput and high packet drop rate. Note that the security and privacy are contradicting issues but the most important issues associated with IoV as the information in IoV is transmitted wirelessly where any vehicles could be malicious (when authentication using vehicle's identity) is not used. Furthermore, when vehicle's identity is used to authenticate the vehicle/driver, privacy of the driver/owner will be at risk. Thus it is essential to have trade-off between security and privacy in IoV.

III. System Model and Problem Statement

A typical system model for the proposed approach is shown in Fig. 1. IoV for smart transportation system consists of networks of smart vehicles equipped with computing, storage and communications devices. Smart vehicles provide communication services among themselves and/or with RSIs using 5G or V2V. Vehicles are assumed to be exchanging the periodic status messages with their neighbors 10 times a second as per the vehicular communication standard [3]. Depending on the type of applications, vehicles could broadcast, multi-cast or unicast their data. Vehicles are assumed to use routing protocols for application such as finding parking spot before getting to the parking lot in an adaptive manner using IoV. Furthermore, each vehicle is assumed to be running an algorithm to prepare the list of trustworthy and malicious vehicles using public key without using any privacy information based on their interactions. Specifically, our system model comprises three components for IoV: i) certificate authority (CA) which maps vehicle's publicly available info such as number plates with cartographic keys using ECC; ii) each vehicle runs malicious vehicle (MV) detection algorithm which works based on trust level calculated using periodic status messages exchanged and other interactions; and iii) each vehicle helps to find a secure Optimal Path (OP) in an adaptive manner based on the intent of communications using ACO-AODV that avoids malicious vehicles.

With this setup, our goal is to design, develop and evaluate an approach that provides both security and privacy by using vehicle's publicly available information (such as number plate of the vehicle) with cryptographic keys and disregarding malicious vehicles by detecting them while finding the best data route in IoV.

IV. Proposed Approach

A. 5G technology in IOV

With the ubiquity of smart terminals and the rapid growth of network traffic, there is a clear indication of requiring 5G technology and its evolution. With the advancement of 5G, the network capacity and spectral efficiency, need to be continually improved, to enhance the user experience a wider variety of communication techniques and approaches need to be provided. Recently, the Internet of Vehicles technology has got ubiquitous attention in the industry for its potential to improve the performance of the smart transportation system and enhance the user experience. With 5G-based IOV communication, based on proposed ACO-AODV best path routing protocol, legitimate data can be directly transmitted between vehicles without routing via RSIs and core network.

Vehicle to vehicle communication helps increase spectral efficiency, expand communication applications, and enhance the user experience:

- Spectral efficiency increased: The legitimate data is directly transmitted between vehicles without routing through a core network and thus results in hop gain. Moreover, resources between vehicles and between vehicle networks and core networks can be reused, and this results in resource reuse gain. With the resource reuse gain and hop gain, network throughput and wireless spectral efficiency can be increased.
- Communication applications expanded: If the communication system collapses due to damage in core network facilities, the IOV model based on 5G communication makes it possible for communication between vehicles to set up ad hoc network and if the vehicles are not covered by a wireless network, multi-hop vehicle to vehicle can be used for further communication.
- User experience enhanced: As technologies develop, short-distance data sharing between nearby vehicles, the location-based services for local users will become a

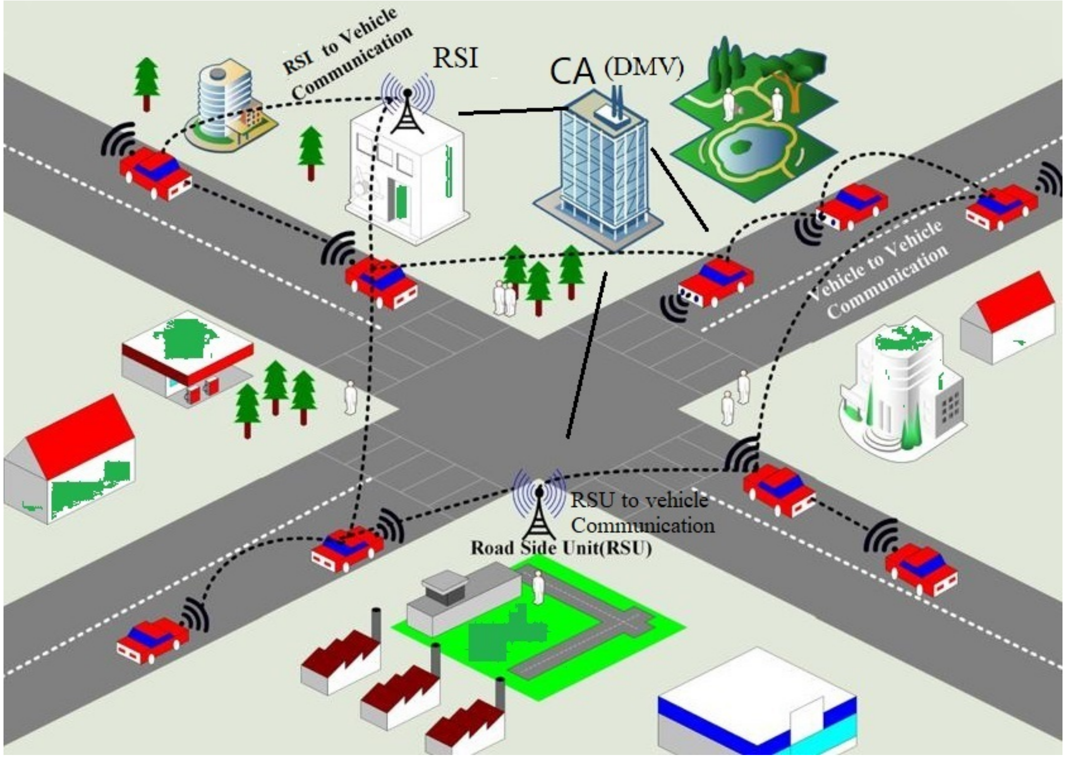
RSI to Vehicle Communication
RSI
CA (DMV)
Vehicle to Vehicle Communication
RSU to vehicle Communication
Road Side Unit(RSU)

Fig. 1. Typical Intent-based Internet of Vehicles (IoV) scenario with certificate authority, RSIs, vehicles and vehicular network where vehicles disregard the data paths with malicious vehicle(s).

significant source of business growth on the wireless platform. The IOV technology based on the 5G network will enhance user experience in these service modes.

B. Certificates Authority (CA) and Key Generation

We consider the third party such as the Department of Motor Vehicles (DMV) in the US as certificate authority (CA) to map the vehicle's number plate (which is a publicly visible unique number and does not violate the privacy of the owner/driver) to public-private key pair using ECC. CA is accountable for the management of the vehicles' number plate, mapping of their identities with the pair of cryptographic keys, and corroborating the misbehavior reports sent by the verifier vehicles and in case found true, changing the distrust value of vehicles. Then the CA generates a certificate for every vehicle that is registered within a network, in addition, upholds key pairs along with certificates of vehicles. An RSU and the DMV will be able to determine whether the misbehavior vehicles has a valid number plate and CA has issued a certificate, thus helping to prevent users' privacy. In this scheme, privacy is preserved as long as the RSU can be trusted. In the key generation, the ECC requires fewer computational power and memory as contrasted with other crypto-systems. Elliptic Curve Cryptography (ECC) can be applied to the dynamic network of IoV using high speed 5G technology as the ECC decreases the complexity of the network and overall size of the data packet by decreasing key size without compromising with the security of the network. The ECC is modified for enhancing the security for IoV by considering secret shared key for secure vehicular communications (as shown in Fig. 2).The public-private pair of keys are used to communicate to a given vehicle by many vehicles or vice versa with an accountability feature. Note that periodic messages (containing <<*vehicle's speed, location, direction and a message encrypted with private key for authenticity of the vehicle*>>) are broadcasted about 10 times a second in IoV. Furthermore, the message encrypted with a given vehicle's private key for authenticity of the message/vehicle can be decrypted with vehicle's public key and check the legitimacy of the message/vehicle. A typical elective curve for ECC is expressed as

$$y^2 = x^3 + ax + b \text{ (mod } p) \qquad (1)$$

where a and b are the integers that satisfy the ECC properties $4a^3 + 27b^2 \neq 0$ (to avoid singular points) [14]. Domain parameters for ECC are listed in Table I. Pair of public-private keys for vehicles and shared secret key for two vehicles can be generated using the steps following.

TABLE I
DOMAIN PARAMETERS FOR ECC

Symbols	Description
p	Field (modulo p)
a, b	Curve Parameters
$G = (X_G, Y_G)$	Generator Point in the Curve
n	Order of G
h	Co factor (with an ideal value = 1)

Suppose vehicle A and B want to communicate with each other and both vehicles want to secure the authenticity and integrity of their messages. Vehicle A pick a private key α, where $1 \leq \alpha \leq n-1$. Similarly, vehicle B picks a private key β, where $1 \leq \beta \leq n-1$. The attacker cannot know α and β. Now vehicle A has both private key α as well as generator G by which calculates its own public key $A = \alpha.G$. Similarly, vehicle B has private key β as well as generator G by which calculates its own public key $B = \beta.G$. Then, vehicle B sends its public key B to vehicle A, then vehicle A receives $B = (X_B, Y_B)$ and Vehicle A sends its public key A to vehicle B, then vehicle B receives $A = (X_A, Y_A)$. So shared secret key between two vehicles is vehicle A compute the shared secret key is $P = \alpha\beta G$ and vehicle B compute the shared secret key is $P = \beta\alpha G$. This way attacker has no idea of private and secret shared keys of both the vehicles.

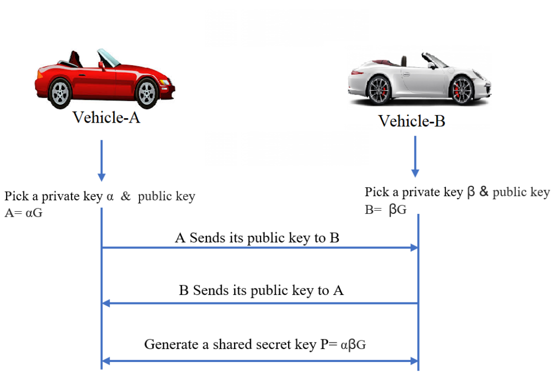
Vehicle-A
Vehicle-B
Pick a private key α & public key
A= αG
Pick a private key β & public key
B= βG
A Sends its public key to B
B Sends its public key to A
Generate a shared secret key P= αβG

Fig. 2. Public key, private key and Secret key generation using ECC.

C. Malicious Vehicle Detection

This section presents an approach that detects malicious vehicles by using the periodic messages or other regular communications.

TABLE II
SYMBOLS AND DESCRIPTION

Symbols	Description
P	Probability
γ_v	Signal to noise ratio
P_{γ_v}	Probability of error
$\hat{\phi}_v$	Trust level
$\mathcal{O}_t$	Observation period
λ_t	Trust threshold level
M	Malicious vehicle
H	Honest vehicle
$\mathcal{Q}$	Set of queries
$\Delta\eta$	Pheromone increment
ω_{ij}	Desirability of transition
ρ	Rate of pheromone evaporation
SV	Source vehicle
DV	Destination vehicle

We consider that $m_v(t)$ is the legitimate information or message by a vehicle v in IoV at time slot t. Malicious vehicles are those vehicles who change the message as $m_v(t) \pm \delta_v$ where δ_v message is either added or removed from the legitimate message $m_v(t)$. In order to increase the accuracy of the proposed approach, we consider each vehicle wait for a couple of interactions (such as 6 periodic status message exchange interactions out of 10 interactions that happen in a second) to classify the vehicle as malicious. For N interacting vehicles for a given road segment and for given observation period $\mathcal{O}_t$, we define the suspicion level of a given vehicle v as Bayesian criterion as

$$\pi_v(t) = \frac{P(\mathcal{O}_t|T_v = M)P(T_v = M)}{\sum_{m=1}^{N} P(\mathcal{O}_t|T_m = M)P(T_m = M)} \tag{2}$$

where T_v and T_m represent malicious vehicle ‘M’ or honest vehicle ‘H’.

Furthermore, when instantaneous signal-to-noise-ratio (SNR), γ_v, is lower than its minimum threshold SNR, $\overline{\gamma}_v$, there will be error in received messages. Thus we take it into account by considering probability of error (because of lower instantaneous SNR than the needed minimum threshold) which is computed as

$$P_{\gamma_v}(t) = Pr\{\gamma_v < \overline{\gamma}_v\} = 1 - Pr\{\gamma_v \geq \overline{\gamma}_v\} \tag{3}$$

The suspicion level caused by intentional change of message and low quality of received signal can be rewritten as

$$\pi_v(t, \gamma_v) \quad = \quad \pi_v(t) \times P_{\gamma_v}(t) \tag{4}$$

Then, the trust level $\hat{\phi}_v(t, \gamma_v)$ of a given vehicle can be computed from its suspicion level as

$$\hat{\phi}_v = \hat{\phi}_v(t, \gamma_v) = 1 - \pi_v(t, \gamma_v) \tag{5}$$

Note that when the trust level $\hat{\phi}_v(t, \gamma_v)$ is lower than the chosen threshold, the given vehicle will not be counted for finding routing path for data when AODV is used for routing. Based on the analysis presented above, the algorithm for detecting malicious vehicle (or finding trustworthy vehicles) is stated as the *Algorithm 1*.

Algorithm 1 Malicious Vehicle Detection and Finding Trustworthy Vehicles)

```
Input: periodic status messages from $N$ participating vehicles and trust threshold level $\lambda_t$, $\mathcal{V}_m = \{\emptyset\}$, $\mathcal{V}_t = \{\emptyset\}$,
repeat
    for each vehicle $v$ do
        Compute $\{\hat{\phi}_v\}_{v=1}^{N}$ based on interactions in IoV.
        if $\hat{\phi}_v < \lambda_T$ then
        Vehicle $v$ is untrustworthy.
        $\mathcal{V}_m = \mathcal{V}_m \cup v$
        else
        Vehicle $v$ is trustworthy.’
        $\mathcal{V}_t = \mathcal{V}_t \cup v$
        end if
    end for
until message is exchanged in IoV
Output:Malicious & trustworthy vehicles: $\mathcal{V}_m \cap \mathcal{V}_t = \{\emptyset\}$.
```

We studied blackhole attack malicious behavior in our proposed malicious detection method. A black hole problem means that one malicious vehicle utilizes the routing protocol to claim itself of being the shortest path to the destination vehicle but drops the routing packets and does not forward packets to its neighbors. A black hole attack easily happens in IoV network. The aims of the proposed trust model are to deal with vehicles who change behavior every time, vehicles who send wrong data, and in addition malicious vehicles.

It is worth noting that the trustworthy vehicles are considered while finding the best route for the data transmission and malicious vehicles are disregarded while finding the data routes using proposed ACO-AODV (which is discussed in the next section).

D. Ant Colony Optimization AODV (ACO-AODV) Routing

Ad hoc On-demand distance vector (AODV) is a reactive protocol consist of route discovery and route maintenance. AODV uses traditional routing tables, one entry per destination, and sequence numbers to verify the update of routing information in route tables and prevents avert routing loops. AODV has the advantage of minimizing the routing table size and broadcast process as routes are created on-demand.

In ACO-AODV, the AODV is improved by using ACO for identifying the best path between source vehicle and destination vehicle. Note that, periodic status messages in IoV are broadcast in nature but there are some applications such as finding parking spot (in the destination location before reaching there) need to use routing protocol such as ACO-AODV. Out of available routes using ‘path request’ and ‘path answer’, the best route is selected using Ant Colony Optimization with AODV for IoV. Algorithm for ACO is illustrated in *Algorithm 2*.

Algorithm 2 ACO algorithm

```
Input: All Routes for Data Communications in IoV.
Output: Best Routing for Data in IoV.
repeat
    repeat
        for each ant/data do
            Choose the next vehicle $v \in \mathcal{V}_t$ by applying the state transition rule and AODV.
            Update pheromone using (6) and (10).
        end for
    until All data routing paths are explored.
    Choose the best routing path for data in IoV.
until Routing is needed.
```

ACO traveling salesman problem is a typical adaptive algorithm since it can transfer information from past environments to a new environment and quickly adapt to dynamic changes. In addition, ACO has strong robustness and handles extreme conditions reasonably. ACO traveling salesman can afford dynamic routing in the Internet of Vehicles.

The ACO algorithm’s main objective was to effectively solve the traveling salesman problem, whose target is to discover the shortest/best route to link multiple vehicles. In ant system, every ants build their respective routes and put their pheromone on their traveled trails. The probability p_{ij}^k of an ant (routing request(RREQ)) k moving from a vehicle i to another vehicle j is expressed as

$$p_{ij}^k = \begin{cases} \frac{\eta_{ij}^{\alpha} \cdot \omega_{ij}^{\beta}}{\sum_{l \in \mathcal{V}_t} \eta_{il}^{\alpha} \cdot \omega_{il}^{\beta}}, & \text{for } i, j \in \mathcal{V}_t \\ 0, & \text{otherwise} \end{cases} \tag{6}$$

where $\mathcal{V}_t$ denotes the set of trusted vehicles which could be visited by ant/data k; η_{ij} denotes the concentrations of pheromone (inversely proportional to delay and distance) between vehicles i and j, ω_{ij} indicates desirability of transition from i to j; and the parameters $\alpha(\geq 0)$ and $\beta(\geq 0)$ represent relative importance of η_{ij} and ω_{ij} respectively. Once the all data routes are built, their pheromone trails are updated. The pheromone value is decreased to forget the formerly taken bad decisions. The pheromone η_{ij} between vehicle i and j is updated as

$$\eta_{ij} = \hat{\phi}_j (1-\rho) \eta_{ij} + \sum_{k=1}^{|\mathcal{Q}|} \Delta\eta_{ij}^k, \qquad \forall i, \forall j \in \mathcal{V}_t, \quad k \in \mathcal{Q} \tag{7}$$

where $\mathcal{Q}$ represents a set of queries/ants, ρ $(0 \leq \rho \leq 1)$ represents the rate of pheromone evaporation and $\hat{\phi}_j$ is the trust level of the vehicle j that determines whether the vehicle j is selected for the next hop or not by the vehicle i. $\Delta\eta_{ij}^k$ is the pheromone deposited by the kth RREQ/ant for a path from vehicle i to j with

$$\Delta\eta_{ij}^k = \begin{cases} \frac{1}{S^k}, & \text{if direct link } i \in \mathcal{V}_t \text{ and } j \in \mathcal{V}_t \text{ is used.} \\ 0, & \text{otherwise} \end{cases} \tag{8}$$

where S^k is the cost of the link/trail between vehicle i and vehicle j in IoV.

The pheromone update mechanism of elite ants is defined as:

$$\eta_{ij} = \hat{\phi}_j (1-\rho) \eta_{ij} + \sum_{k=1}^{|\mathcal{Q}|} \Delta\eta_{ij}^k + \Delta\eta_{ij}^{best} \tag{9}$$

$\Delta\eta_{ij}^{best}$ is pheromone increment of elite ants which on the path from vehicle i to j with

$$\Delta\eta_{ij}^{best} = \begin{cases} \frac{1}{S^{best}}, & \text{if best link } i \in \mathcal{V}_t \text{ and } j \in \mathcal{V}_t \text{ is used.} \\ 0, & \text{otherwise} \end{cases} \tag{10}$$

Fig. 3 shows a typical process of a route discovery of the proposed ACO-AODV routing protocol. The source SV sends the RREQ (Route Request) to the neighboring vehicles using red arrow. In-turn, these vehicles send the RREQ to their adjacent vehicle and this whole process goes on until it gets to the destination DV. Note that each vehicle neglects the untrustworthy vehicles such as MV1 and MV2 (identified by Algorithm 1), as shown in Fig. 3 for potential data route. After receiving that RREQ, the DV sends the RREP (Route Reply) to its neighboring vehicles and the process goes on till it reaches the source vehicle SV. Note that the route is selected which has least delay, no malicious vehicles along the route and shortest path in terms of number of vehicles between SV to DV.

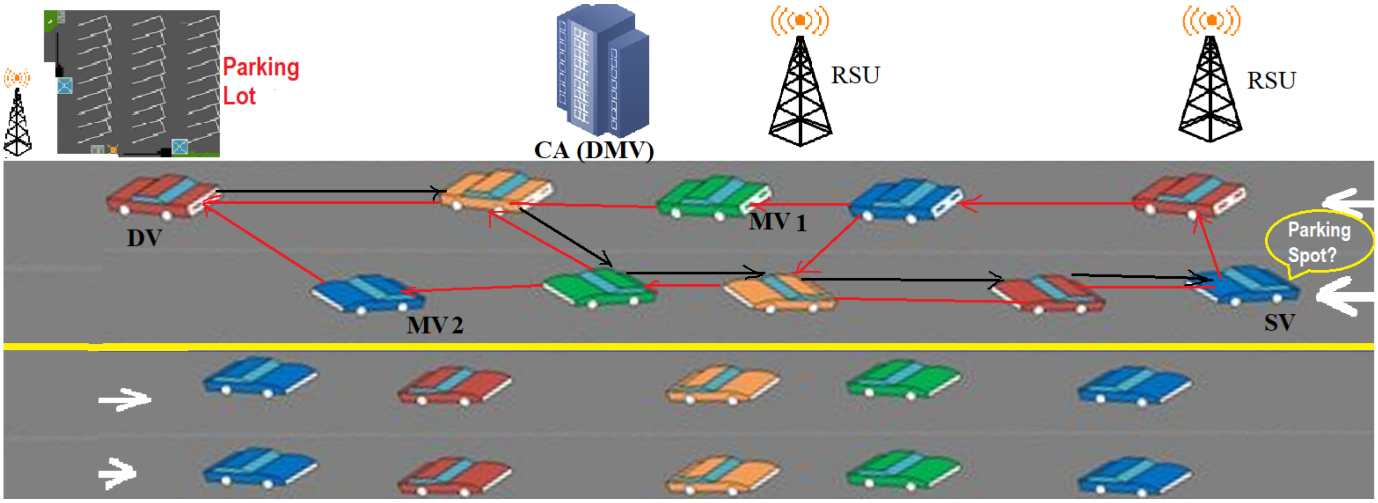

Fig. 3. Route discovery for the ACO-AODV routing protocol where source vehicle (SV) is querying to destination vehicle (DV) about parking spot using multi-hop vehicular communications. Route Request (RREQ)- red line from SV to DV, and Route Reply (RREP) - black line from DV to SV shows the best route for data communications where malicious vehicles MV1 and MV2 are excluded from the route.

V. Performance Evaluation and Discussion

The performance of the proposed ECC based ACO-AODV protocol is evaluated using extensive simulations. We used the Matlab based simulator that was designed and developed by the authors. We consider a road segment of 1 miles with three lanes with 100 to 500 vehicles where vehicles' speeds are generated using normal distribution with mean 60 mph ± 40 mph of variance [26]. Small percentage of vehicles is randomly chosen to act as malicious ones by either dropping packets or reporting fake information for periodic status messages. Vehicles are assumed to maintain safety separation distance by using periodic status messages and run the proposed algorithms to find trustworthy vehicles and best data route from source vehicle to destination vehicle. We have compared the performance of the proposed ACO-AODV protocol with two other protocols called SE-AOMDV [17] and AODV [19] by considering expected end-to-end delay, per-vehicle throughput, packet drop rate and routing overhead by varying the number of vehicles or speed of the vehicles in IoV.

First, we plotted the expected delay vs the number of vehicles in IoV, as shown in Fig. 4, which gives the average period taken to deliver the data from the source vehicle (SV) to the destination vehicle (DV) and vice versa. Furthermore, we plotted the expected delay for two other protocols: AODV and SE-AOMDV protocol, as shown in Fig. 4. Expected delay increases with increasing number of vehicles since there will be more routes and packets will have to traverse through more number of vehicles. Furthermore, Fig. 4 shows that the proposed ACO-AODV protocol gives lower expected delay than that of exiting SE-AOMDV and AODV protocols since our approach considers only trusted vehicles with lower congestion along the data route.

Next, we plotted the expected packet drop rate vs the number of vehicles in IoV for the proposed ACO-AODV protocol and two state of the art protocols, as shown in Fig. 5. The expected packet drop rate shows how many packets were sent from source vehicle and how many were successfully received at the destination vehicle for given time. Fig. 5 shows that the packet drop rate increases with the increasing number of vehicles in IoV. However, the proposed ACO-AODV results in lowest packet drop rate compared to state of the art protocols: SE-AOMDV and AODV, as shown in Fig. 5, since our protocol selects the node with high trust and least congestion for routing.

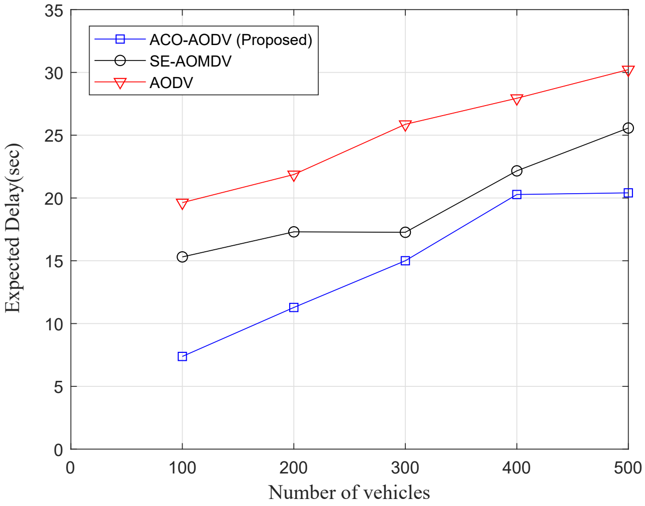

Fig. 4. Comparison in terms of expected delay vs the number of vehicles for the proposed ACO-AODV and the existing SE-AOMDV and AODV protocols.

Next, we plotted expected throughput vs the number of vehicles for the proposed ACO-AODV and existing SE-AOMDV and AODV protocols, as shown in Fig. 6. The proposed ACO-AODV outperforms the existing protocols, as shown in Fig. 6. Next, we plotted the expected throughput vs the average speed of the vehicle, as shown in Fig. 7 where we observed that the proposed approach outperforms the existing approaches. Note that, per-vehicle throughput decreases with increasing number of vehicles, as shown in Fig. 6, because of increasing

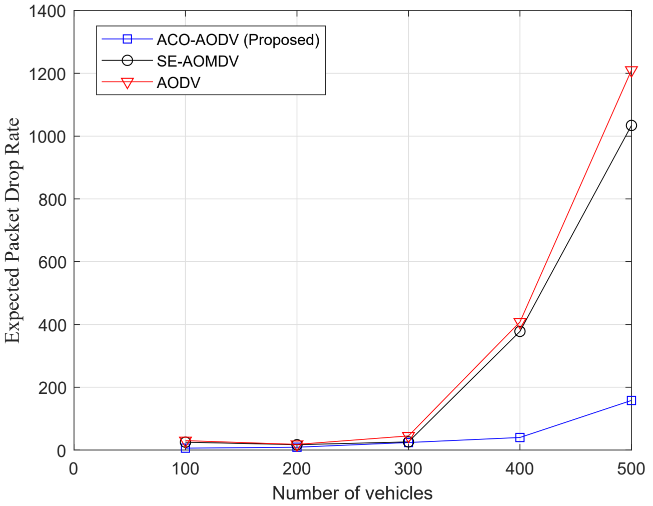

Fig. 5. Expected packet drop rate of proposed approach and existing approaches [17], [19].

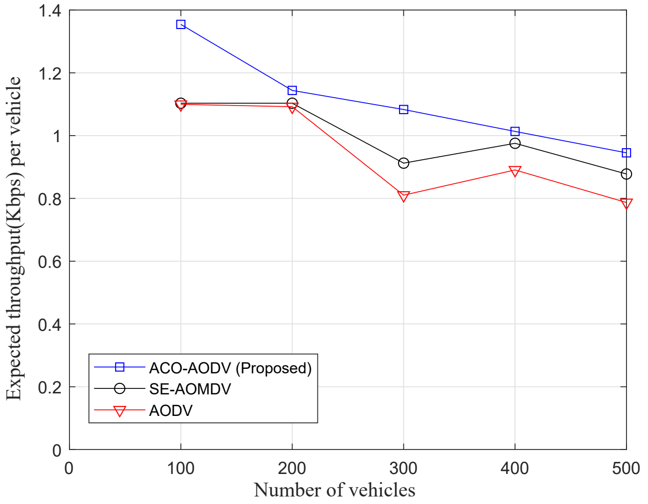

Fig. 6. Expected throughput vs the number of vehicles for the proposed approach and existing approaches [17], [19].

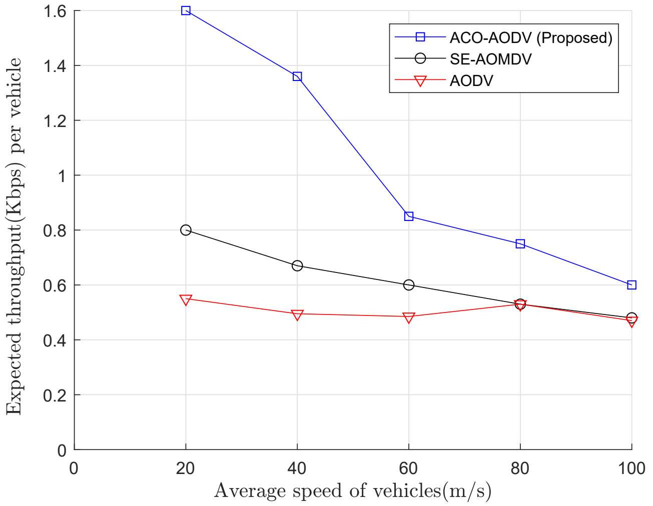

Fig. 7. Variation of expected throughput vs the average speed of the vehicles for proposed approach and existing approaches [17], [19].

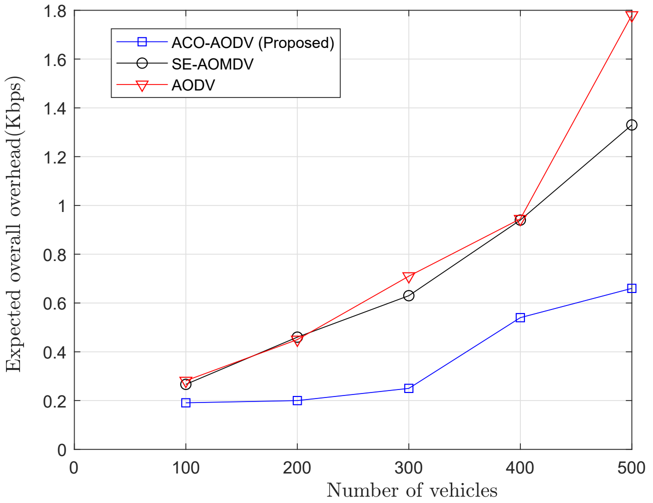

Fig. 8. Expected routing overall overhead vs the number of vehicles for the proposed approach and existing approaches [17], [19].

competition for transmission opportunities and with increasing speed as shown in Fig. 7. This is mainly because of change in network topology in IoV caused by high speed vehicles.

Later, we plotted the expected routing overhead (which is based on total number of control or routing packets needed for a given routing protocol) vs the number of vehicles, as shown in Fig. 8. Overall expected routing overhead is significantly lower for the proposed ACO-AODV protocol than that of existing protocols, as shown in Fig. 8. Our proposed ACO-AODV protocol disregards suspicious vehicles and considers trustworthy vehicles as candidate for routing path, which helps reduce the overall routing overhead, as shown in Fig. 8.

Then, we plotted expected packet delivery ratio (PDR) vs the number of vehicles for the proposed ACO-AODV and existing SE-AOMDV and AODV protocols, as shown in Fig. 9. Next, we plotted the expected PDR vs the average speed of the vehicle, as shown in Fig.10. For efficient transmission, the packet delivery ratio should be high. If the PDR has the highest value then, all the information is obtained at the receiver without any loss. From Fig 9, it is obvious that the proposed approach attains the highest PDR value. And from Fig 10 the proposed approach gives higher PDR value than the existing approaches.

Finally, we plotted expected packet delivery ratio with respect to percentage of malicious vehicle in Fig.11, the packet drop rate keeps increasing until it reaches approximately 158 in the worst case when malicious node percentage is more than or equal to 87% and all malicious nodes are blackhole attackers where they drop all the received packets. Moreover, we measured the network throughput as shown in Fig.12 and we notice that our model, in the case of the blackhole attack, the network performance decreases to reach 0.8 in the worst

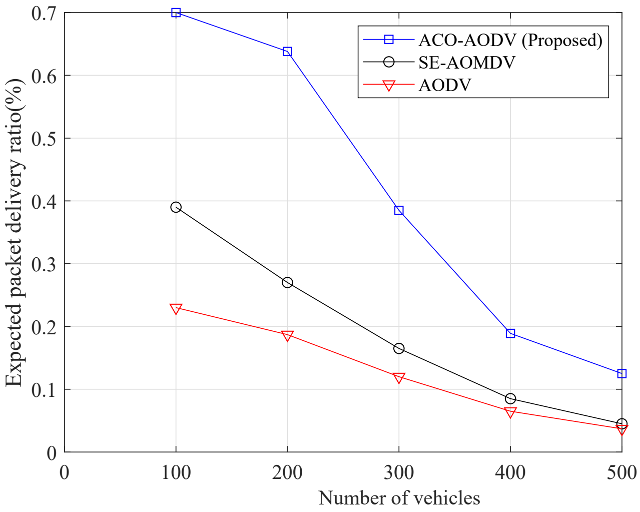

Fig. 9. Expected packet delivery ratio vs the number of vehicles for the proposed approach and existing approaches [17], [19].

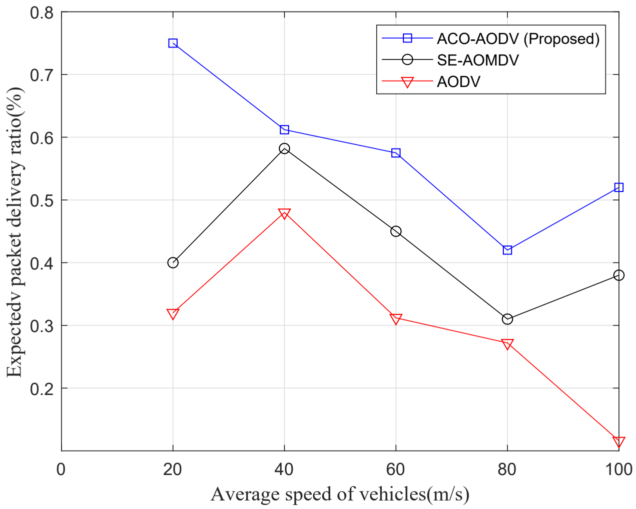

Fig. 10. Expected packet delivery ratio vs average speed of the vehicles for the proposed approach and existing approaches [17], [19].

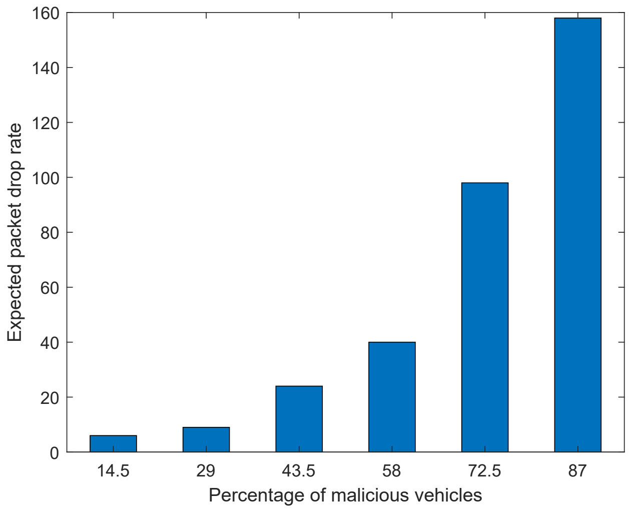

Fig. 11. Variation of expected packet drop rate vs the percentage of malicious vehicles.

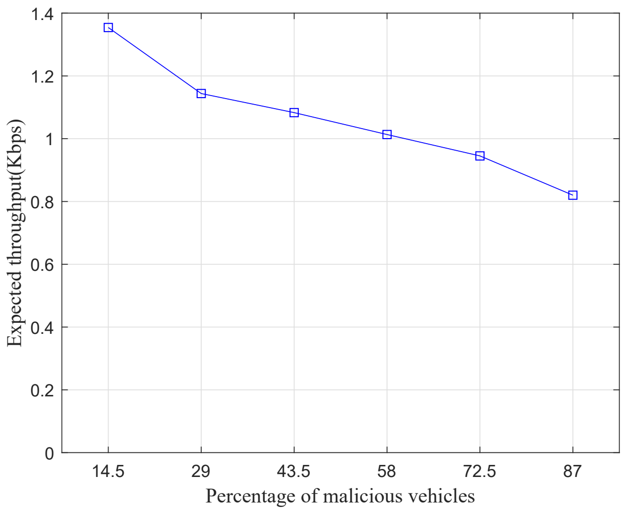

Fig. 12. Variation of expected throughput vs the percentage of malicious vehicles.

case when there is high percentage of malicious nodes.

VI. Conclusion

IoV is regarded as the backbone for smart transportation system for smart city applications that relies on moving vehicles to form a mobile ad hoc network on the road. Routing in IoV is one of the hardest tasks because of the high mobility of vehicles. Furthermore, secure and privacy-aware routing is more challenging in vehicular network since vehicles are linked with owners'/drivers' private information. Because of the contradicting nature of security (based on authentication) and privacy (based on hiding identities), it is very hard to achieve both at the same time and there is no standard protocol for IoV available yet for this. In this paper, we have proposed an ECC based privacy-aware secure ACO-AODV routing protocol for IoV. Specifically, the proposed approach leverages the certificate authority that maps vehicle's publicly available information to ECC keys, detects and avoids malicious vehicle by using their periodic interactions, and finds the optimal path by using ACO-AODV routing protocol. The performance of the proposed approach is evaluated by using extensive simulation results. Numerical results illustrate that the proposed ACO-AODV routing protocol provides higher throughput, lower delay and lower routing overhead compared to the closely related state of the art approaches.

Acknowledgments

This work was supported in part by the US NSF under grants CNS 1650831 and HRD 1828811, and by the U.S. Department of Homeland Security under grant DHS 2017-ST-062-000003 and by the DoE's National Nuclear Security Administration (NNSA) Award # DE-NA0003946. However, any opinion, finding, and conclusions or recommendations expressed in this document are those of the authors and should not be interpreted as necessarily representing the official policies, either expressed or implied, of the funding agencies.

References

[1] Neeraj Kumar, Sudip Misra, Joel JPC Rodrigues, and Mohammad S Obaidat, "Coalition games for spatio-temporal big data in Internet of vehicles environment: a comparative analysis," *IEEE Internet of Things Journal*, vol. 2, no. 4, pp. 310-320, 2015.

[2] Wenjia Li and Houbing Song, "ART: An attack-resistant trust management scheme for securing vehicular ad hoc networks," *IEEE Trans. on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 960–969, 2015.

[3] S. Olariu and M. C. Weigle, *Vehicular networks: from theory to practice*. Chapman and Hall/CRC, 2009.

[4] Kazi Masudul Alam, Mukesh Saini, and Abdulmotaleb El Saddik, "Toward social internet of vehicles: Concept, architecture, and applications," *IEEE Access*, vol. 3, pp. 343-357, 2015.

[5] Mario Gerla, Eun-Kyu Lee, Giovanni Pau, and Uichin Lee, "Internet of vehicles: From intelligent grid to autonomous cars and vehicular clouds," Pro. of the *IEEE World Forum on Internet of Things*, pp. 241-246, 2014.

[6] Zaid Abdulkader A, Azizol Abdullah, Mohd Taufik Abdullah, and Zuriati Ahmad Zukarnain, "Malicious node identification routing and protection mechanism for vehicular ad-hoc network against various attacks," *International Journal of Networking and Virtual Organizations*, vol. 19, no. 2-4, pp. 153-175, 2018.

[7] Sunilkumar Manvi S, and Shrikant Tangade, "A survey on authentication schemes in VANETs for secured communication," Vehicular Communications, vol. 9, pp. 19-30, 2017.

[8] Philippe Golle, Dan Greene, and Jessica Staddon, "Detecting and correcting malicious data in VANETs," In Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks, pp. 29-37, 2004.

[9] Xue Yang, Leibo Liu, Nitin H. Vaidya, and Feng Zhao, "A vehicle-to-vehicle communication protocol for cooperative collision warning," In The First Annual International Conference on Mobile and Ubiquitous Systems: Networking and Services, pp. 114-123, 2004.

[10] Chia Hoou, "A roadside unit-based localization scheme for vehicular ad hoc networks," International Journal of Communication Systems, vol. 27, no. 1, pp. 135-150, 2014.

[11] Vinh Hoa La and Ana Rosa Cavalli, "Security attacks and solutions in vehicular ad hoc networks: a survey," 2014.

[12] Shunrong Jiang, Xiaoyan Zhu, and Liangmin Wang, "An efficient anonymous batch authentication scheme based on HMAC for VANETs," IEEE Transactions on Intelligent Transportation Systems, vol. 17, no. 8, pp. 2193-2204, 2016.

[13] N. Kumar, S. Misra, J. J. Rodrigues, and M. S. Obaidat, "Coalition games for spatio-temporal big data in internet of vehicles environment: a comparative analysis," *IEEE Internet of Things Journal*, vol. 2, no. 4, pp. 310–320, 2015.

[14] D. Hankerson, A. J. Menezes, and S. Vanstone, *Guide to elliptic curve cryptography*. Springer Science & Business Media, 2006.

[15] Xiaoyan Zhu, Shunrong Jiang, Liangmin Wang, and Hui Li, "Efficient privacy-preserving authentication for vehicular ad hoc networks," IEEE Transactions on Vehicular Technology, vol. 63, no. 2, pp. 907-919, 2013.

[16] Wei Liu and Ming Yu, "AASR: authenticated anonymous secure routing for MANETs in adversarial environments", IEEE Transactions on Vehicular Technology, vol. 63, no. 9, pp. 4585-4593, 2014.

[17] Amel Meddeb Makhlouf and Mohsen Guizani, "SE-AOMDV: secure and efficient AOMDV routing protocol for vehicular communications," International Journal of Information Security, PP. 1-12, 2019.

[18] Rasheed Hussain and Heekuck Oh, "On secure and privacy-aware sybil attack detection in vehicular communications," Wireless personal communications, vol. 77, no. 4, pp. 2649-2673, 2014.

[19] Tyagi, P., Dembla, D.: Performance analysis and implementation of a proposed mechanism for detection and prevention of security attacks in routing protocols of a vehicular ad-hoc network (VANET). Egypt. Inform. J. 18(2), 133–139 (2017).

[20] Chaker Abdelaziz Kerrache, Abderrahmane Lakas, Nasreddine Lagraa, and Ezedin Barka, "UAV-assisted technique for the detection of malicious and selfish nodes in VANETs," Vehicular Communications, vol. 11, pp. 1-11, 2018.

[21] Hamssa Hasrouny, Abed Ellatif Samhat, Carole Bassil, and Anis Laouiti, "Trust model for secure group leader-based communications in VANET," Wireless Networks, pp. 1-23, 2018.

[22] Kevin Bylykbashi, Donald Elmazi, Keita Matsuo, Makoto Ikeda, and Leonard Barolli, "Effect of security and trustworthiness for a fuzzy cluster management system in VANETs," Cognitive Systems Research, vol. 55, pp. 153-163, 2019.

[23] Danda B. Rawat, Chandra Bajracharya, "Vehicular Cyber Physical Systems: Adaptive Connectivity and Security," Springer 2016.

[24] Mingzhong Wang, Dan Liu, Liehuang Zhu, Yongjun Xu, and Fei Wang, "LESPP: lightweight and efficient strong privacy preserving authentication scheme for secure VANET communication," Computing, vol. 98, no. 7, pp. 685-708, 2016.

[25] Zhong, Hong, et al. "Efficient conditional privacy-preserving and authentication scheme for secure service provision in VANET." Tsinghua Science and Technology 21.6 (2016): 620-629.

[26] D. B. Rawat and C. Bajracharya, "Vehicular Cyber Physical Systems: Adaptive Connectivity and Security," Springer, 2017.

[27] Wang, Jian, et al. "A trust propagation scheme in VANETs." 2009 IEEE Intelligent Vehicles Symposium, 2009.

[28] Li, Xiaoqing, et al. "RGTE: A reputation-based global trust establishment in VANETs." 2013 5th International Conference on Intelligent Networking and Collaborative Systems. IEEE, 2013.

[29] Bißmeyer, Norbert, et al. "Central misbehavior evaluation for vanets based on mobility data plausibility." Proceedings of the ninth ACM international workshop on Vehicular inter-networking, systems, and applications. 2012.

[30] Mármol, Félix Gómez, and Gregorio Martínez Pérez. "TRIP, a trust and reputation infrastructure-based proposal for vehicular ad hoc networks." Journal of network and computer applications 35.3 (2012): 934-941.

[31] Huang, Junqin, et al. "Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism." IEEE Transactions on Industrial Informatics 15.6 (2019): 3680-3689.

Sunitha Safavat received has been working towards her PhD in Computer Science under the supervision of Dr. Danda B. Rawat in the Department of Electrical Engineering and Computer Science (EECS) at Howard University, Washington DC, USA. Her research interests include Internet-of-Vehicles, Mobile Edge Computing, software-defined systems and Cybersecurity. She is a member of Cybersecurity and Wireless Networking Innovations (CWiNs) Lab and a member of the Data Science and Cybersecurity Center(DSC2) at Howard University, USA.

Danda B. Rawat (IEEE Senior Member) received his Ph.D. degree from Old Dominion University, Norfolk, Virginia, USA. Dr. Rawat is a Professor in the Department of Electrical Engineering and Computer Science, Founder & Director of the Data Science and Cybersecurity Center, Director of CWiNs Lab and Graduate Program Director of CS Graduate Programs at Howard University, Washington, DC, USA. Dr. Rawat is engaged in research and teaching in the areas of cybersecurity, machine learning and wireless networking for emerging networked systems including cyber-physical systems, Internet-of-Things, smart cities, software defined systems and vehicular networks. His professional career comprises more than 15 years in academia, government, and industry. He has secured over $5 million in research funding from US National Science Foundation, US Department of Homeland Security, Department of Energy, National Nuclear Security Administration (NNSA), DoD Research Labs, Industry (Microsoft, Intel, etc.) and private Foundations. Dr. Rawat is the recipient of NSF CAREER Award in 2016, Department of Homeland Security (DHS) Scientific Leadership Award in 2017, the US Air Force Research Laboratory (AFRL) Summer Faculty Visiting Fellowship in 2017, Outstanding Research Faculty Award (Award for Excellence in Scholarly Activity) at GSU in 2015, the Best Paper Awards and Outstanding PhD Researcher Award in 2009. He has delivered over 15 Keynotes and invited speeches at international conferences and workshops. Dr. Rawat has published over 200 scientific/technical articles and 9 books. He has been serving as an Editor/Guest Editor for over 30 international journals. He has been in Organizing Committees for several IEEE flagship conferences such as IEEE INFOCOM, IEEE CNS, IEEE ICC, IEEE GLOBECOM and so on. He served as a technical program committee (TPC) member for several international conferences. Dr. Rawat is a Senior Member of IEEE and ACM, a member of ASEE and AAAS, and an IET Fellow.