IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received September 8, 2018, accepted September 30, 2018, date of publication October 15, 2018,
date of current version November 14, 2018.

Digital Object Identifier 10.1109/ACCESS.2018.2875906

Trust-Based Distributed Authentication Method for Collision Attack Avoidance in VANETs

AMR TOLBA
Computer Science Department, Community College, King Saud University, Riyadh 11437, Saudi Arabia
Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Kom 32511, Egypt
e-mail: atolba@ksu.edu.sa

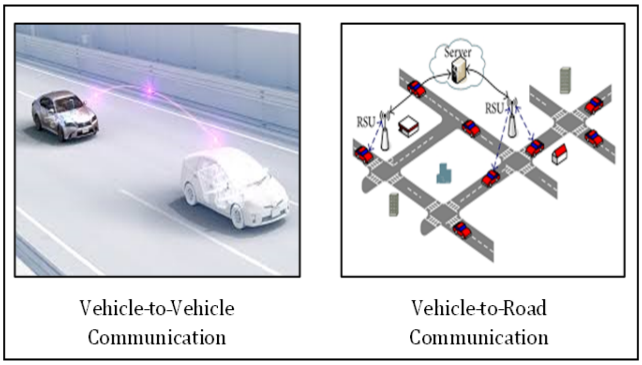
This work was supported by King Saud University, Deanship of Scientific Research, Community College Research Unit.

ABSTRACT A vehicular ad hoc network (VANET) is a collection of mobile vehicles that aids roadside communication through vehicle-to-vehicle and vehicle-to-infrastructure operation modes. The network is autonomous and, hence, requires a wide range of security measures to protect its communications from attack. Recent studies on VANET security have focused on resolving the issues due to computation and distribution density of the vehicles. Probability distribution measures have been administered for detecting collision attacks, which increases the computational complexity. In this paper, a trust-based distributed authentication (TDA) method that relies on a global trust server and vehicle behavior for avoiding collision attacks is proposed. This method ensures both inter-vehicular and intra-vehicular communication security in the network. In addition, a channel state routing protocol (CSRP) is proposed to improve the communication reliability among the vehicles. Reliable vehicles are identified according to the on-board unit (OBU) energy and the channel state of the vehicle to deliver seamless communication. The biased methods are assimilated to improve the communication reliability by avoiding collision attacks and improving secured packets flow in VANETs. In particular, the CSRP minimizes the energy exploitation of OBUs and time delay. TDA improves the security of the network by improving the collision recognition rate and the broadcast rate.

INDEX TERMS Vehicular ad-hoc networks, mobile ad-hoc networks, collision attacks, trust hash-based, channel state routing protocol.

I. INTRODUCTION

Vehicular ad-hoc networks (VANETs) are the foundation of next-generation intelligent transportation systems (ITSs), which are a subset of mobile ad-hoc networks (MANETs). MANETs aim to provide inter-vehicle communication and roadside-to-vehicle communication to increase the safety and efficiency of roads by providing precise and useful data to drivers and road specialists [1], [2]. VANETs aim to enhance wide variety of applications, including road and security applications, for example, notifications of traffic congestion, emergency notifications, and peer-to-peer communications for sharing information. Performing channel estimation and the according routing can significantly improve VANETs [3]. According to the various applications, VANETs have been used to create intelligent systems through vehicle-to-vehicle (V2V) communication [4]. This vehicle-based communication process relies on the density of receivers and actions. From the obtained vehicle communication, the VANET manages the roadside unit (RSU) used to transmit information from one vehicle to another. The transmitted messages help to control the VANET [5] and establish the intelligent transport system in a successful manner. According to the discussions, the V2V communication process is shown in Fig. 1.



Vehicle-to-Vehicle Communication

Vehicle-to-Road Communication

FIGURE 1. VANET communication in vehicles.

During the vehicle communication process, the VANET maintains different characteristics [6], such as the prediction concept, geographical communication, dynamic topology, mobility node, and frequency node changing process. These characteristics are used to determine the efficiency of vehicular communication. Even though the network has several characteristics, the network congestion and channel allocation are major issues because the routing decision of vehicle communication is difficult. Thus, different routing protocols [7], such as the routing information protocol, enhanced interior gateway routing protocol, and distance-vector routing protocol, are introduced for avoiding network congestion. The routing protocol helps to detect the optimized route for transmitting the message from one node to another in an effective manner but faces several issues, such as route disconnections and high node densities, which affect the entire V2V communication process. Several studies have been conducted in this area. Network assignment for channel allocation and stable routing methods was performed for mobile cognitive networks by using an integrated transmission cost and relay workload, resulting in optimized routing [8], [9]. The reliable routing technique introduced in [10] depends on the energy cost, minimum energy, and lifetime of the network. However, without consideration of the channel state (CS) and resource allocation, the routing is compromised. Thus, this paper introduces an energy-optimization technique based on a CS routing protocol with trust-based distributed authentication (CSRP-TDA) to eliminate intermediate collision attacks and maintain the network in an effective manner.

II. RELATED WORK

To address the aforementioned issue, resource allocation with flexible channel cooperation through optimization based on Nash bargaining systems was designed [11]. Collision detection and correction are two of the major difficulties to be overcome in ITSs. In [12], randomized network structuring and a packet routing framework based on nearest-neighbor communications improved the energy consumed per packet. In [13], resource allocation with multiple relays was designed, with the aid of a greedy algorithm that improved the end-to-end rate. One of the main issues in the workflow management system is the proper and optimal allocation of resources. Discrete optimization was applied to reduce the computational complexity, and the system workload was designed in [14], this model is defined to minimize the energy expenses of the network. In [15], the vehicular network communication process is managed by applying an interaction collision warning system (ICWS) for eliminating network collisions as well as intermediate attacks. During the communication process, the network utilizes a three-dimensional ray launching algorithm for managing the V2I communication, which minimizes the path loss and collision attacks effectively. In [16], cooperative message authentication protocol (CMAP)-based optimized smart cities were created by a vehicular cyber physical system. During the development process, the system utilized several roadside access points, along with shopkeepers, which attract passing customers. An evaluation scheme using a cooperative awareness message was presented to address issues related to the collision probability. Furthermore, a distributed key management framework for reducing the computational overhead in VANETs was presented. Due to the openness of the ad-hoc network, launching attack or malicious nodes are natural in VANETs. This is accomplished through intermittent monitoring of the network. Among the various types of attacks, the collision attack is significant because of its open nature. An overview of security approaches for VANETs was presented in [17] and [18]. More challenges are involved in secure and efficient exchange of information in VANETs than for any other type of ad-hoc network. A reliable broadcast protocol based on a disjunctive code was presented in [19], increasing the rates of transmission and reception in the VANET. An attack-resilient mix zone was presented in [20], ensuring the location privacy of mobile users in an intermittent manner. An interruption recognition framework for security in a basic medicinal framework was introduced in [21] and [22] according to the control determination-based Intrusion Detection System procedure. One of the most popular research topics in the field of cryptography is the application of the privacy-preserving data aggregation problem.

In [23]–[26], a privacy preservation scheme using a sum and product based on the aggregation model was investigated, which minimized both the communication and computational complexities. One of the growing types of attacks in the internet community is the malware attack. In [27], optimal distributed malware defense using content-based signatures was investigated, with the aim of ensuring security and a high data broadcast rate. This study considers safe correspondence in remote sensor systems in view of a new dynamic versatile limited-time chaos synchronization approach considering noise and vulnerability [28]. For this reason, the adjustments proposed in [29] are applied to the base station and sensor hubs to create tumultuous signs. Confused signs are influenced by noise and vulnerability. Initially, the modified segment examination is performed to isolate the clamor from the disorderly flags. At this point, by utilizing the versatile limited-time sliding-mode controller, a control law and a versatile parameter-tuning strategy are proposed for accomplishing limited-time confusion synchronization under the uproarious conditions and parametric vulnerabilities. Synchronization between the base station and each of the sensor hubs is acknowledged through confused flag [27]–[30]. Reproduction is introduced to demonstrate the adequacy and pertinence of the proposed system. Thus, the most efficient information gathering algorithm for the associated target scope involves expanding the wireless sensor network (WSN) lifetime, for both static and versatile multi-hop WSNs [31]–[36]. In [34], a privacy preserving framework for cloud is designed. It preserves the end-user privacy in a distributed manner. In this work, collision attack detection using trust-based hash is used to ensure a reliable and functional VANET communication. Collision attack correction is used for motivating vehicles to participate in secure data-packet transmission and for increasing the availability and quality of the network. The proposed method protects the data packets by using vehicle- and message-level model to ensure a high collision attack detection rate without significant delay.

The main contributions of this paper are as follows.

1. A novel collision attack detection and avoidance system with low energy consumption employing the optimized routing method of CSRP-TDA is proposed.
2. A CS routing protocol (CSRP) is designed for improving the communication rates of the vehicles and reducing the delay. CS-based routing improves the energy efficiency of the on-board units (OBUs) by curtailing energy exploitations.
3. The TDA design prevents collisions causing attacks from participating in the routing process.
4. The TDA further administers security for V2V and V2I communications with the help of a global trust server and hashed messages.
5. The two methods are integrated to improve the energy efficiency of the OBUs, the broadcast rate, and the collision recognition, as well as to minimize the time delay in communication.

This paper is organized as follows. The Introduction and Related Work are presented in Sections I and II, respectively. Section III presents the operations of the CSRP and TDA for implementation. Section IV details the experimental settings. Section V presents the NS2 simulation results. Section VI gives concluding remarks.

III. MATERIALS AND METHOD

A. NETWORK MODEL

Consider a vehicular network with V vehicles that move independently using Manhattan Mobility. The vehicles are equipped with a sensor that builds the OBU of vehicular communications. The sensors are intended to gather information from their neighbors and relay this information to a distant sink node or base station. The vehicles in the network communicate with their neighbors through a bi-directional link E; the network can be expressed as a graph of $G = (V, E)$. A vehicle communicates with the sink node by relying on its neighbors; the links are augmented for communication, as indicated by (1).

$$V = \sum V_s \cup V_{sn} \tag{1}$$

Here, V_s and V_{sn} represent the source and sink vehicles, respectively. Two vehicles V_i and V_j are said to be in-range if (2) is satisfied.

$$d\left(V_i, V_j\right) < R(V_i||V_j) \tag{2}$$

Here, $d\left(V_i, V_j\right)$ is the distance between the two vehicles, and R is the communication range of the vehicles.

B. CSRP

The CSRP relies on the CS of the neighbor and the remaining energy of the OBU. The communicating source vehicle initiates a CS request to its neighbors; the neighbors acknowledge either CS = 0 (idle) or CS = 1 (busy). The source vehicle selects a set of all vehicles V with CS $= 0$ and computes d and the residual energy (E_R) of its neighbors. If E_i and E_c are the initial energy and the energy consumption of the OBU, respectively, the residual energy of the OBU is calculated using (3).

$$E_R = E_i - E_c \tag{3}$$

Then, the CSR factor (CSRF) for identifying an optimal neighbor is computed using (4).

$$CSRF = min(E_R) * min(d) \tag{4}$$

A neighbor with the maximum CSRF is selected as the next optimal vehicle for transmission. The optimality of the vehicle based on the CSRF is verified after each set of communication based on d and E_R. As the velocity of the vehicles changes with time, the distance between the sink and the source varies. It is not essential that the same neighbor must be available during different transmission sequences.

In this routing, the vehicle initiates a request/acquires data if the CS of the neighbor is idle [37]–[39]. For seamless communication, if the CS is busy, the active communicating source searches for a new neighbor to pursue further transmissions. Fig. 2, illustrates the flow of the proposed CSRP.

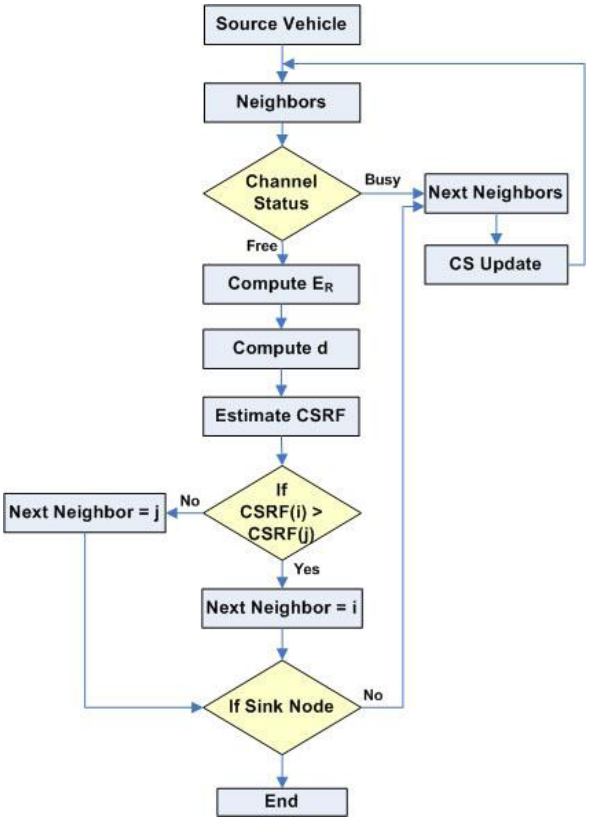


FIGURE 2. Flow diagram of the CSRP.

The source vehicle reaches the sink node in either one hop or multiple hops. For multi-hop communication, the source relies on its neighbors to reach the destination. On each communication assessment of visiting a neighbor node, the process is continued until the sink is reached. The CSRF is updated through the series of observations. The proposed CSRP protocol classifies vehicles as neighbors (CV = 0) or sinks (CV = 1).

1) CONTRARY ANALYSIS

Two or more neighbors are selected with CS = 0 and even energy levels.

2) SOLUTION

In this case, the distance between the neighbor and the sink is assessed for identifying the closest neighbor. Unlike the conventional methods, the shortest distance from the neighbor to the sink is considered in selecting the optimal vehicle. An ideal sink location that ensures optimal energy utilization is represented by (5).

$$(x_{sn}, y_{sn}) = min\left\{\sqrt{(x_i - x_{sn})^2 + (y_i - y_{sn})^2}, \sqrt{\left(x_j - x_{sn}\right)^2 + \left(y_j - y_{sn}\right)^2}, \ldots\right\} \quad (5)$$

Algorithm 1 CSRP

```
    For ¥ V in X ∗ Y
        IF (d(vi, vj) ≤ R(v))
            Best (cs_req)
            IF (cs = = 1)
                Compute ER using (3)
                Compute CSRF using (4)
                    IF (CSRF(i) > CSRF(i))
                        Next_vehicle = i
                    Else
                        Next_vehicle = j
                    End if
                CV = 0;
                    If (CV = 1)
                        Deliver date packet;
                    End if
                    End if
                End if
        End For
```

Algorithm 1, describes the process of the proposed CSRP protocol. The collected data are relayed through available neighbors that satisfy both the channel and energy constraints. This optimality in the neighbor selection is employed throughout the relaying process to improve data collection rates and to reduce overhead. The energy of the forwarding vehicle is acquired through periodic update messages. The energy-insufficient OBU vehicles are discarded from the handling information; thus, premature energy failures are prevented, minimizing the redundant energy exploitation. If the number of users is increasing, the channel response algorithm [40], [41] can be incorporated with the proposed CSRP to minimize the exchange of control messages.

C. TRUST-BASED DISTRIBUTED AUTHENTICATION (TDA)

In this section, the proposed TDA model, that identifies any collision attack on the VANET, is described. Fig. 3 shows a block diagram of the TDA model. The model consists of three main phases: (i) the Training phase, (ii) the Collision Attack Detection phase, and (iii) the Collision Correction phase. An elaborate description of each phase is presented in Fig. 3.

1) TDA–TRAINING PHASE

In the Training phase, which is considered the most time-consuming phase, the TDA extracts the features representing the network statistical behavior. The communication time, source, neighbor information and the packet type are the features extracted in this phase. The process is confined with legitimate vehicles alone. In the TDA, the features are directly extracted from the bit stream of a corresponding data packet, which does not need to be decoded at the other end, aiming at reducing the time- consuming process while the features are extracted. The occurrences of the bit stream in a data packet that includes 64-bit positions are taken into account. Hence, the data-packet vector DPV_0 is given as

$$DPV_0 = \{DPV\,(X_0)\,, DPV\,(X_1)\,, \ldots.., DPV\,(X_{63})\}\,. \qquad (6)$$

Here, $DPV\,(X_i)$ represents the possibility of bit stream "1" appearing at the i^{th} bit position. Then, the data-packet vector is reduced from DPV to DPV_r and the feature vector fv at time interval t is generated, as follows:

$$fv\,(n) = DPV_r\,(n) \oplus DPV_r\,(n-1)\,. \qquad (7)$$

Here, $\oplus$ symbolizes the exclusive-or operator, which represents the bit position of the data-packet vector. The vector-based training algorithm is denoted as Algorithm 2.

Algorithm 2 Vector-Based Training

```
    Input: Data packets '$DP = DP_1, DP_2, \ldots, DP_n$',
           Normal packet '$NP = NP_1, NP_2, \ldots, NP_n$',
           Attack packet '$AP = AP_1, AP_2, \ldots, AP_n$',
           Data-packet vector '$DPV_0$'
    Output:Computationally efficient data-packet vector
    Begin
        For each data packet '$DP$'
            Extract data-packet vector '$DPV_0$' using (6)
            Reduce data-packet vector from '$DPV$' to '$DPV_r$'
            using (7)
        End for
    End
```

The packets are classified based on the grade and trust of the vehicle. The most recent trust and grade value of a vehicle determines the type of packet being circulated.

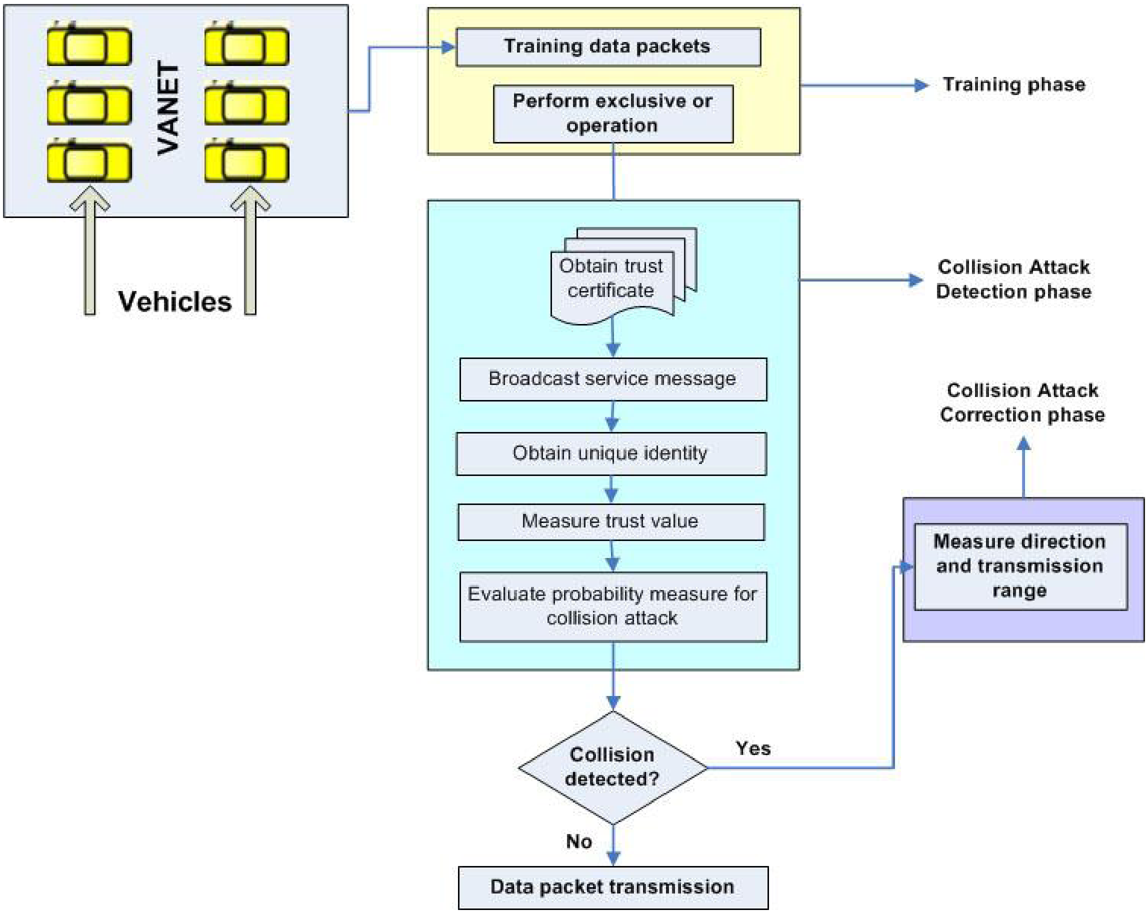

VANET
Vehicles
Training data packets
Perform exclusive or operation
Training phase
Obtain trust certificate
Broadcast service message
Obtain unique identity
Measure trust value
Evaluate probability measure for collision attack
Collision Attack Detection phase
Collision Attack Correction phase
Measure direction and transmission range
Collision detected?
Yes
No
Data packet transmission

FIGURE 3. Block diagram of TDA.

As shown in Algorithm 2, for each data packet, the vector-based training algorithm is designed with the objective of reducing the collision detection time by extracting a computationally efficient data-packet vector. Owing to the high time complexity involved in the extraction, the TDA extracts the features directly from data-packet vector using the exclusive-or operator. The collision attack detection using the trust-based hash model with the generated data-packet vector is discussed in the following subsections [42]–[44].

2) TDA—COLLISION ATTACK DETECTION PHASE

As shown in Fig. 4, the network involved in TDA comprises three entities: the vehicles, RSUs, and servers. Every vehicle in the network broadcasts and receives messages through ad-hoc communication. Data packets are carried by each vehicle, with each vehicle acting as a service provider through which the data packets are transmitted from source to destination. The RSU, being a wireless communication device, connects to the servers for secure communication between the vehicles and servers. The TDA also has a trust server to maintain the vehicle trust and issue trust certificates.

As shown in Fig. 4, whenever a source vehicle V_P needs to send a data packet (DP) to a destination vehicle V_Q, the source vehicle must obtain a trust certificate (TC) from the trust server (TS):

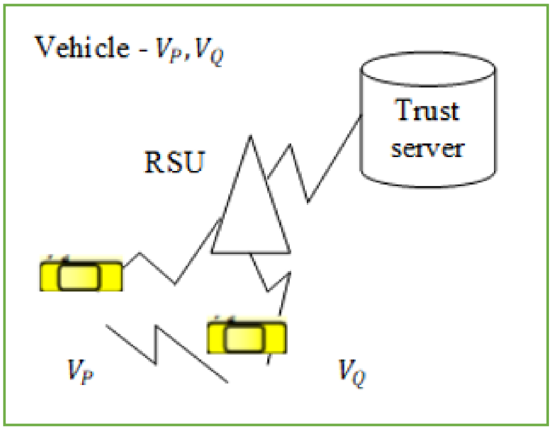


FIGURE 4. Trust-based VANET model.

$$TC = (DP, TV, TS_{ID}) . \tag{8}$$

Here, the TC comprises the DP, the trust value (TV), and the identification (ID) of the TS, i.e., TS_{ID}. Once the trust certificate is obtained by the source vehicle, it broadcasts a service message (SM), along with the trust certificate. The service message is given as

$$SM = (TC, E, V_{ID}) . \tag{9}$$

Here, the service message includes the trust certificate TC obtained from the trust server, an event E (an instance), and the vehicle ID, i.e., V_{ID}. Whenever an event occurs, a unique event identity (EID) is generated using a hash function:

$$Hash\,(DP_1, DP_2) \rightarrow (SK_P, SK_Q). \tag{10}$$

The event identifier decides if the vehicle has a communication or a request phase to handle. To limit fake request message generation, the EID is broadcasted to the requesting neighbors for verification. Upon receipt of the message by the vehicle V_Q, the signatures are verified, and the trust value of V_P is obtained. The TS gathers the response messages, groups the trust values, and updates the accounts of the source and destination vehicles (V_P and V_Q, respectively). The TS maintains the vehicle record as "$(V_{ID}, TV\ (SM)\ , G)$", where V_{ID} represents the unique vehicle ID intended to send the data-packet vector maintained by the TS, $TV\ (SM)$ represents the service message trust value for the unique vehicle V_{ID}, and G represents the grade. The grade of the vehicle is used to assess its reliability towards trust. The reliability is estimated with the communication characteristics of the vehicle.

Malicious vehicles (i.e., colliding vehicles) purposefully send the TDA assumes that false service messages. A low service trust value indicates a colliding vehicle.

Algorithm 3 Trust-Based Hash

```
Input: Data packets ‘DP =DP_1,DP_2, ...,DP_n’, Trust
Server ‘TS’
Output: Collision attack detection
Begin
    For each data packet ‘DP’
    Source vehicle sends data-packet vector along with
    the feature vector to the trust server
    Creation of trust value by trust server using (8)
      For each event
        Generate service message using (9)
        Generate unique event identity through hash
        function using (10)
        Obtain data packet vector using (6)
      End for
    End for
End
```

As shown in Algorithm 3, for each data-packet vector, sent by the source vehicle to the destination vehicle, the trust-based hash algorithm initially proceeds with the assumption that the falsification of data packets is created by malicious vehicles for their own advantage. The service trust value is modeled for every vehicle, which identifies the malicious or colliding vehicles that give low quality services. For collision attack detection, the TDA uses mathematical modeling to measure the position where the minimum criteria are satisfied to safeguard the vehicles in the VANET. The location coordinates of the new vehicle and the existing vehicles are obtained. A threshold value of the radius R is obtained. With this measure (i.e., the location coordinates and threshold radius value), the coordinates within the threshold radius are considered to represent an authentic vehicle. The selected vehicles are used for secure communication. In contrast, the coordinates that lie outside the threshold radius are considered to represent a non-authentic vehicle and associated with the colliding node. The vehicles with low TC levels are discarded from communication. The TS updates the reliability of the communicating vehicle with the help of recommendations from its neighbors.

Hence, the proposed CSRP-TDA method brings significant improvements in the broadcast rate, with controlled delay and better security. The vehicles that are not authentic are denied from communication process, the interference and overhearing energy for their verification is conserved. The trust model with the base originality benchmark prevents the colliding nodes from accessing the vehicular network, and results indicate that collision detection and correction using TDA has a considerably better success rate.

3) TDA–COLLISION ATTACK CORRECTION PHASE

The correction process is carried out with any of the existing methods like Aloha detection or any other mitigation methods [42]–[44].

Many novel methods have been proposed for collision attack and detection in the past. In this paper, the link stability and energy-aware routing are presented to solve the bi-objective optimization formulation, improving the normal vitality utilization by means of the CSRP and the system lifetime. The proposed framework was intended to guarantee protection of the information to be transmitted in the VANET. At the point when various servers send information to a similar beneficiary in a parallel way, in-cast congestion is said to occur. To address this issue, a congestion avoidance system was designed that ensures not only zero timeouts but also high throughput in data center networks with secured data transmission through TDA. While all these studies assume a cooperative message authentication scheme, in the present study, energy-aware routing with a collision attack detection and correction model to achieve security and a high broadcasting rate in the presence of colliding vehicles is developed with energy consumption and end-to-end delay to deliver packets between vehicles, ensuring reliable communication. TDA enhances the security of VANET communications using trust certificates and hash binding. The trust certificate ensures the selection of a legitimate vehicle, and the hash-based event occurrence improves the message security.

IV. EXPERIMENTAL SETTINGS

The TDA model used in the VANET employs the NS2 simulator with a network range of 1,400 m × 1,400 m. The experimental parameter settings are shown in Table 1.

TABLE 1. Parameter settings.

Parameters	Values
Simulator	NS 2.34
Network Region	1,400 m × 1,400 m
Simulation time	1,500 s
Density of nodes	10, 20, 30, 40, 50, 60, 70
Size of data packet	100–512 bytes/packet
Transmission range of the vehicles	40 m, 80 m, 100 m

Experimental analysis is performed on the parameters, such as the broadcast rate, security, and collision attack detection rate, with respect to the vehicle density in the VANET. The TDA metrics model is compared with the ICWS [15] and CMAP [16], [42] in the VANET.

V. RESULTS AND DISCUSSION

The advantages and efficiency of the CSRP-TDA model in the VANET with the ICWS and CMAP, along with the parameters of the TDA, were analyzed using NS2. The analysis of the proposed method is described as follows.

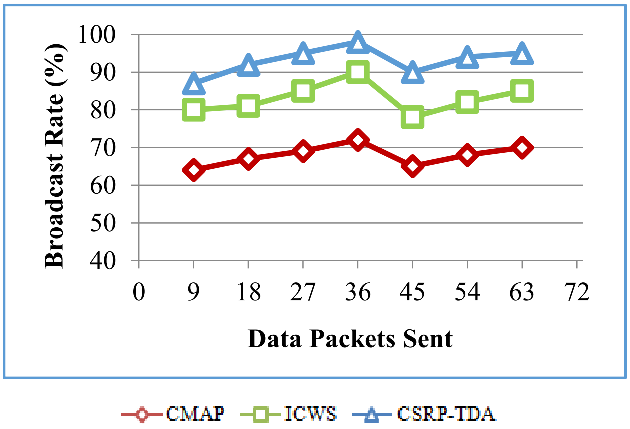


FIGURE 5. Broadcast rate based on the data packets.

The broadcast rate for data packets sent in the VANET is shown in Fig. 5, and the proposed CSRP-TDA is compared with the existing ICWS and CMAP. The broadcast rate is improved in the TDA model because the collision attack is detected at an early stage by applying the trust-based hash model. By applying the trust-based hash model in CSRP-TDA, the broadcast rate is ensured through a TS that maintains the trust certificate, which along with the service message ensures secure transmission. This enhances the communicate rate by 9% compared with the ICWS. The unique event identity generated for each vehicle further enhances the broadcast rate in CSRP-TDA. Information packets are safely transmitted to the receiver end with the awareness of attacker location. This enhances the communication rate by 23% compared with the CMAP.

As shown in Fig. 6, for the vector-based training algorithm, applying the exclusive-or operator to each position of bits in position vectors results in the improvement of the collision time, ensuring better security. The number of packets secured over the transmitted data packets, in the proposed CSRP-TDA is high. .In the CSRP-TDA model, with the features extracted directly from the bit stream, decoding is not required at the receiving end, improving the rate of security in the CSRP-TDA model by 12% compared with the ICWS and 23% compared with the CMAP. In addition, with the application of the trust model and the colliding node removal process, VANET can handle stronger attacks.

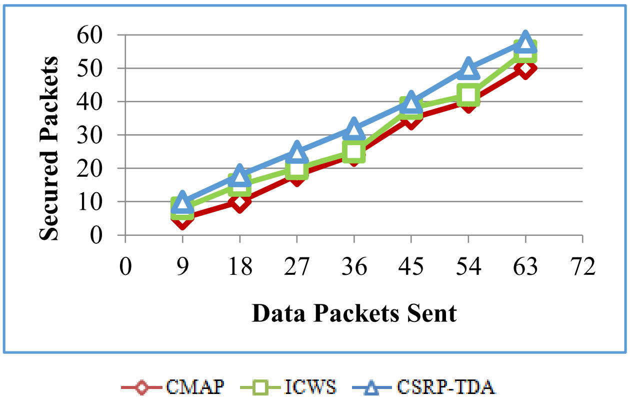


FIGURE 6. Measurement of the security.

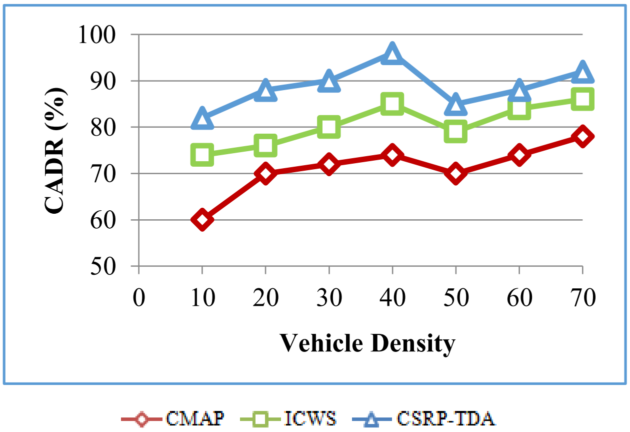


FIGURE 7. Measurement of the collision attack detection rate (CADR).

Fig. 7 shows the variation of the collision attack recognition rate for unusual exercises regarding the vehicle density in the VANET. Each of the outcomes shown in Fig. 7, affirms that the proposed CSRP-TDA method essentially overcomes the other two techniques: the ICWS and CMAP. The collision-rate abnormal activity is enhanced in the CSRP-TDA model using the trust certificate issued by the TS, which generates a service message. This generated service message with a single event identity obtained through the hash function, improves the collision attack detection rate. As a result, the collection attack detection rate is improved by 9% compared with the ICWS. Moreover, the probability measurement obtained with a unique identity through the hash function improves the collision attack detection rate using the CSRP-TDA model by 18% compared with the CMAP.

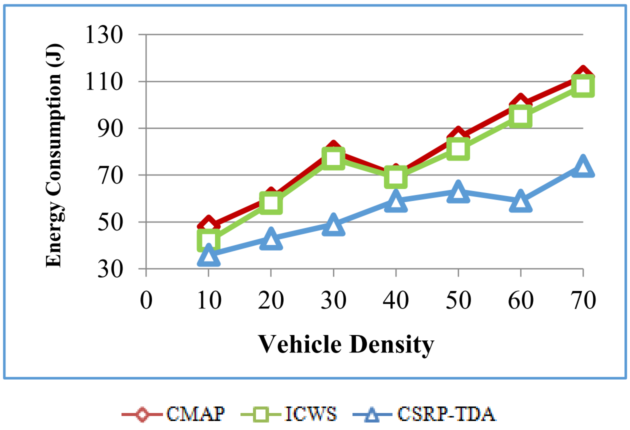


FIGURE 8. Measurement of the energy consumption.

Fig. 8 compares the energy consumption of the sink node for CSRP-TDA with those for the ICWS and CMAP. Here, the CSRP employs optimal combination of minimum distance, remaining energy, and CS for each OBU. This improves the success rate of data collection at the sink node, reducing the total energy consumption.

Furthermore, the CSRP utilizes recursive verification for ideal information gathering, and the sensor hubs are positioned along the optimal route to finish the information collection. This technique can reduce the workload of information gathering and hence minimizes the aggregate energy cost.

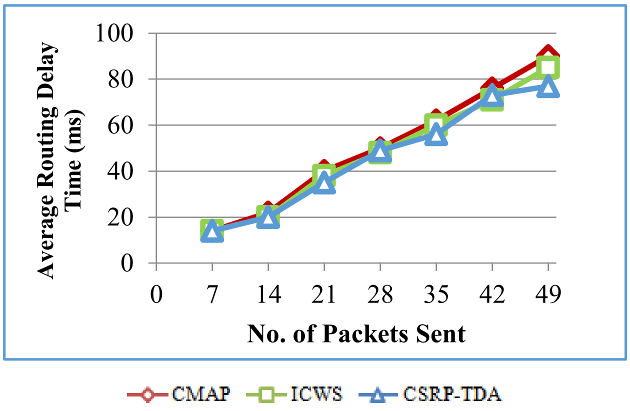


FIGURE 9. Average routing delay time.

Fig. 9 shows the average routing delay time with respect to the number of packets sent. As shown, the average routing delay time (minimal) for CSRP-TDA is shorter than the minimal average routing delay time in the optimal routes found by ICWS and CMAP. This is because, in the CSRP-TDA method, an evaluation standard is designed to verify the performance of the path vehicles. This standard consumes less energy while searching for the optimal route with minimal energy. Thus, the average routing delay time found by CSRP-TDA is the shortest. It was reduced by 4% compared with the ICWS and 8% compared with the CMAP.

VI. CONCLUSION

This manuscript proposes a CSRP with TDA for improving the reliability in VANET communication. The CSRP is intended to select optimal neighbors according to the CS and the energy of the OBUs to sustain communication. TDA ensures security at the vehicle and communication levels independently to retain consistency and authenticity. As the model uses the trust-based algorithm in a dynamic way, it enhances the security, ensuring secure data transmission between vehicles in the VANET. This is achieved through a unique identity for each round of a source vehicle to transmit packets. Subsequently, the proposed algorithm performs secure information packet transmission, diminishing the end-to-end delay, and overcomes the overhead in the VANET. Simulations are performed to test the security, broadcast rate, and collision attack detection rate with respect to the vehicle density. The results indicate that CSRP-TDA offers better execution, with improvements of 16% and 17% in the communication rate and security, respectively, than ICWS and CMAP separately.

ACKNOWLEDGMENT

The author would like to thank the Deanship of Scientific Research and RSSU at King Saud University for their technical support.

REFERENCES

[1] S. Boussoufa-Lahlah, F. Semchedine, and L. Bouallouche-Medjkoune, "Geographic routing protocols for vehicular ad hoc networks (VANETs): A survey," *Veh. Commun.*, vol. 11, pp. 20–31, Jan. 2018.

[2] F. Xia *et al.*, "User popularity-based packet scheduling for congestion control in ad-hoc social networks," *J. Comput. Syst. Sci.*, vol. 82, pp. 93–112, Feb. 2016.

[3] C. Cooper, D. Franklin, M. Ros, F. Safaei, and M. Abolhasan, "A comparative survey of vanet clustering techniques," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 1, pp. 657–681, 1st Quart., 2017.

[4] J. Singh and K. Singh, "Congestion control in vehicular ad hoc network: A review," in *Next-Generation Networks* (Advances in Intelligent Systems and Computing), vol. 638, D. Lobiyal, V. Mansotra, and U. Singh, Eds. Singapore: Springer, 2018.

[5] P. Agarwal, "Technical review on different applications, challenges and security in VANET," *J. Multimedia Technol. Recent Advancements*, vol. 4, no. 3, pp. 21–30, 2018.

[6] R. Sugumar, A. Rengarajan, and C. Jayakumar, "Trust based authentication technique for cluster based vehicular ad hoc networks (VANET)," *Wireless Netw.*, vol. 24, no. 2, pp. 373–382, 2018.

[7] A. Rahim *et al.*, "Social acquaintance based routing in vehicular social networks," *Future Gener. Comput. Syst.*, to be published, doi: 10.1016/j.future.2017.07.059.

[8] A. M. Ahmed *et al.*, "BoDMaS: Bio-inspired selfishness detection and mitigation in data management for ad-hoc social networks," *Ad Hoc Netw.*, vol. 55, pp. 119–131, Feb. 2017.

[9] R. Amin and J. Martin, "Assessing performance gains through global resource control of heterogeneous wireless networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 2, pp. 292–305, Feb. 2016.

[10] X. Liu, Z. Li, P. Yang, and Y. Dong, "Information-centric mobile ad hoc networks and content routing: A survey," *Ad Hoc Netw.*, vol. 58, pp. 255–268, Apr. 2017.

[11] H. Al-Tous and I. Barhumi, "Resource allocation for multiple-sources single-relay cooperative communication OFDMA systems," *IEEE Trans. Mobile Comput.*, vol. 15, no. 4, pp. 964–981, Apr. 2016.

[12] S. Ji, M. Yan, R. Beyah, and Z. Cai, "Semi-structure routing and analytical frameworks for cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 15, no. 4, pp. 996–1008, Apr. 2016.

[13] W.-H. Kuo, W. Liao, and T. Liu, "Adaptive resource allocation for layer-encoded IPTV multicasting in IEEE 802.16 WiMAX wireless networks," *IEEE Trans. Multimedia*, vol. 13, no. 1, pp. 116–124, Feb. 2011.

[14] N. Kumar and Y. Singh, "An energy efficient opportunistic routing metric for wireless sensor networks," *Indian J. Sci. Technol.*, vol. 9, no. 32, pp. 1–7, 2016.

[15] M. Silvestri and F. Bella, "Effects of intersection collision warning systems and traffic calming measures on Driver's behavior at intersections," in *Advances in Human Aspects of Transportation*. Cham, Switzerland: Springer, 2017, pp. 773–786.

[16] W. Shen, L. Liu, X. Cao, Y. Hao, and Y. Cheng, "Cooperative message authentication in vehicular cyber-physical systems," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 1, pp. 84–97, Jun. 2013.

[17] J. Yang, Y. Chen, W. Trappe, and J. Cheng, "Detection and localization of multiple spoofing attackers in wireless networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 24, no. 1, pp. 44–58, Jan. 2013.

[18] C. Ponikwar, and H.-J. Hof, "Overview on security approaches in intelligent transportation systems: Searching for hybrid trust establishment solutions for VANETs," in *Proc. 9th Int. Conf. Emerg. Secur. Inf., Syst. Technol. (SECURWARE)*, 2015, pp. 160–165.

[19] J. Molina-Gil, P. Caballero-Gil, and C. Caballero-Gil, "Countermeasures to avoid noncooperation in fully self-organized VANETs," *Sci. World J.*, vol. 2014, Jun. 2014, Art. no. 589563.

[20] X. Fan, C. Wang, J. Yu, K. Xing, Y. Chen, and J. Liang, "A reliable broadcast protocol in vehicular ad hoc networks," *Int. J. Distrib. Sensor Netw.*, vol. 11, no. 8, p. 286241, 2015.

[21] B. Palanisamy and L. Liu, "Attack-resilient mix-zones over road networks: Architecture and algorithms," *IEEE Trans. Mobile Comput.*, vol. 14, no. 3, pp. 495–508, Mar. 2015.

[22] R. Mitchell and I.-R. Chen, "Behavior rule specification-based intrusion detection for safety critical medical cyber physical systems," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 16–30, Jan./Feb. 2015.

[23] T. Jung, X.-Y. Li, and M. Wan, "Collusion-tolerable privacy-preserving sum and product calculation without secure channel," *IEEE Trans. Dependable Secure Comput.*, vol. 12, no. 1, pp. 45–57, Jan. 2015.

[24] Y. Li, P. Hui, D. Jin, L. Su, and L. Zeng, "Optimal distributed Malware defense in mobile networks with heterogeneous devices," *IEEE Trans. Mobile Comput.*, vol. 13, no. 2, pp. 377–391, Feb. 2014.

[25] Y. Brun and N. Medvidovic, "Entrusting private computation and data to untrusted networks," *IEEE Trans. Dependable Secure Comput.*, vol. 10, no. 4, pp. 225–238, Jul. 2013.

[26] H. Wu, Z. Feng, C. Guo, and Y. Zhang, "ICTCP: Incast congestion control for TCP in data-center networks," *IEEE/ACM Trans. Netw.*, vol. 21, no. 2, pp. 345–358, Apr. 2013.

[27] D. Schürmann and S. Sigg, "Secure communication based on ambient audio," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 358–370, Feb. 2013.

[28] B. Vaseghi, M. A. Pourmina, and S. Mobayen, "Secure communication in wireless sensor networks based on chaos synchronization using adaptive sliding mode control," *Nonlinear Dyn.*, vol. 89, pp. 1689–1704, Aug. 2017.

[29] S. Biswas, R. Das, and P. Chatterjee, "Energy-efficient connected target coverage in multi-hop wireless sensor networks," in *Industry Interactive Innovations in Science, Engineering and Technology*. Singapore: Springer, 2018, pp. 411–421.

[30] E. Y. Vasserman and N. Hopper, "Vampire attacks: Draining life from wireless ad hoc sensor networks," *IEEE Trans. Mobile Comput.*, vol. 12, no. 2, pp. 318–332, Feb. 2013.

[31] Z. Ning, X. Kong, F. Xia, W. Hou, and X. Wang, "Green and sustainable cloud of things: Enabling collaborative edge computing," *IEEE Commun. Mag.*, to be published, doi: 10.1109/MCOM.2018.1700895.

[32] Z. Ning, J. Huang, and X. Wang, "Vehicular fog computing: Enabling real-time traffic management for smart cities," *IEEE Wireless Commun.*, to be published, doi: 10.1109/MWC.2018.1700441.

[33] X. Wang *et al.*, "A city-wide real-time traffic management system: Enabling crowdsensing in social Internet of vehicles," *IEEE Commun. Mag.*, vol. 56, no. 9, pp. 19–25, Sep. 2018, doi: 10.1109/MCOM.2018.1701065.

[34] X. Wang *et al.*, "A privacy-preserving message forwarding framework for opportunistic cloud of things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2864782.

[35] X. Wang, Z. Ning, and L. Wang, "Offloading in Internet of vehicles: A fog-enabled real-time traffic management system," *IEEE Trans. Ind. Informat.*, vol. 14, no. 10, pp. 4568–4578, Oct. 2018, doi: 10.1109/TII.2018.2816590.

[36] L. Guo, Z. Ning, W. Hou, B. Hu, and P. Guo, "Quick answer for big data in sharing economy: Innovative computer architecture design facilitating optimal service-demand matching," *IEEE Trans. Autom. Sci. Eng.*, vol. 15, no. 4, pp. 1494–1506, Oct. 2018, doi: 10.1109/TASE.2018.2838340.

[37] M. Xie, J. Hu, and S. Guo, "Segment-based anomaly detection with approximated sample covariance matrix in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 26, no. 2, pp. 574–583, Feb. 2015.

[38] Y. Chen, S. Nyemba, and B. Malin, "Detecting anomalous insiders in collaborative information systems," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 3, pp. 332–344, May/Jun. 2012.

[39] M. Alsaleh, M. Mannan, and P. C. van Oorschot, "Revisiting defenses against large-scale online password guessing attacks," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 1, pp. 128–141, Jan./Feb. 2012.

[40] K. Xu, H. Xiong, C. Wu, D. Stefan, and D. Yao, "Data-provenance verification for secure hosts," *IEEE Trans. Dependable Secure Comput.*, vol. 9, no. 2, pp. 173–183, Mar./Apr. 2012.

[41] I. Dhyani, N. Goel, G. Sharma, and B. Mallick, "A reliable tactic for detecting black hole attack in vehicular ad hoc networks," in *Advances in Computer and Computational Sciences*. Singapore: Springer, 2017, pp. 333–343.

[42] Y. Hao, Y. Cheng, C. Zhou, and W. Song, "A distributed key management framework with cooperative message authentication in VANETs," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 616–629, Mar. 2011.

[43] H. Liu, X. Bai, Z. Yang, A. Tolba, and F. Xia, "Trust-aware recommendation for improving aggregate diversity," *New Rev. Hypermedia Multimedia*, vol. 21, nos. 3–4, pp. 242–258, 2015.

[44] Z. Ning, P. Dong, X. Kong, and F. Xia, "A cooperative partial computation offloading scheme for mobile edge computing enabled Internet of Things," *IEEE Internet Things J.*, to be published, doi: 10.1109/JIOT.2018.2868616.

AMR TOLBA received the M.Sc. and Ph.D. degrees from the Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Egypt, in 2002 and 2006, respectively. He is currently an Associate Professor with the Faculty of Science, Menoufia University. He is currently on leave from Menoufia University to the Computer Science Department, Community College, King Saud University, Saudi Arabia. He has authored or co-authored over 50 scientific papers in top ranked (ISI) international journals and conference proceedings. His main research interests include socially aware networks, vehicular ad hoc networks, Internet of Things, intelligent systems, big data, recommender systems, and cloud computing. He serves as a technical program committee member in several conferences.