On Detection of Sybil Attack in Large-Scale VANETs Using Spider-Monkey Technique

CELESTINE IWENDI[1]**, (Senior Member, IEEE), MUEEN UDDIN**[ID][2]**, JAMES A. ANSERE**[3]**,
P. NKURUNZIZA**[3]**, J. H. ANAJEMBA**[3]**, AND ALI KASHIF BASHIR**[ID][4]**, (Senior Member, IEEE)**
[1]Bangor College China, Central South University of Forestry and Technology, Hunan 410004, China
[2]Department of Information Systems, Faculty of Engineering, Effat University, Jeddah 22332, Saudi Arabia
[3]College of Internet of Things Engineering, Hohai University, Changzhou 213022, China
[4]Faculty of Science and Technology, University of the Faroe Islands, 100 Tórshavn, Denmark

Corresponding author: James A. Ansere (jaansere@hhu.edu.cn)

ABSTRACT Sybil security threat in vehicular ad hoc networks (VANETs) has attracted much attention in recent times. The attacker introduces malicious nodes with multiple identities. As the roadside unit fails to synchronize its clock with legitimate vehicles, unintended vehicles are identified, and therefore erroneous messages will be sent to them. This paper proposes a novel biologically inspired spider-monkey time synchronization technique for large-scale VANETs to boost packet delivery time synchronization at minimized energy consumption. The proposed technique is based on the metaheuristic stimulated framework approach by the natural spider-monkey behavior. An artificial spider-monkey technique is used to examine the Sybil attacking strategies on VANETs to predict the number of vehicular collisions in a densely deployed challenge zone. Furthermore, this paper proposes the pseudocode algorithm randomly distributed for energy-efficient time synchronization in two-way packet delivery scenarios to evaluate the clock offset and the propagation delay in transmitting the packet beacon message to destination vehicles correctly. The performances of the proposed technique are compared with existing protocols. It performs better over long transmission distances for the detection of Sybil in dynamic VANETs' system in terms of measurement precision, intrusion detection rate, and energy efficiency.

INDEX TERMS Spider monkey time synchronization (SMTS), Sybil attacks, probability of detection, VANETs.

I. INTRODUCTION

The advancements in intelligent vehicular transportation networks brought comfort and efficiency to daily activities. Passengers can reach their destination faster and safer than the traditional transport system. In vehicular ad hoc networks (VANETs) system, there is constant communications among vehicles and the Roadside Units (RSUs), to inform drivers on the current developments on the road in case there is accident or traffic congestion [1]. RSUs must have prior knowledge of the vehicles for proper traffic management information, to ensure sound VANETs deployment on the road [2]. Safer transportation means saving lives since many car accidents have caused great casualties. Many threat Detection protocols for Sybil attack such as privacy preserving detection of abuses of pseudonyms (P2DAP), session key certificate (SKC) and enhanced attacked packet detection algorithm (EAPDA) for detecting the malicious nodes multiple identities that caused Sybil attacks

in VANETs, have been proposed [3]–[5]. However, the existing protocols in practical network topology applications encounter challenges in the detection of Sybil attacks. In both P2DAP and SKC techniques, sensor nodes have high energy consumption due to algorithm complexity and access delays, causing packet beacon message collision among the cluster heads (CHs) and vehicle members. EAPDA only detect the malicious nodes and has an extended propagation delay that compromises throughput and the network security.

Novel synchronized biologically-inspired protocols have been proposed [6], [7]. Few researchers have addressed the communication insecurities in aligning the time division multiple access (TDMA) timeslot for transmission of the information packet that integrates with Chameleon-MAC, which is a self-robust mobility TDMA protocol. Chameleon-MAC boosts channel utilization and energy efficient resources allocation among the network users that share same spectrum [8].

Vehicles attacked by malicious nodes usually cause time synchronization error in beacon message dissemination. This causes propagation delay and beacon message loss. The author's proposed technique mitigates this by employing two detection time synchronization techniques. The inter-vehicle detection phase that avoids collision among beacon messages inside vehicular cluster formed was first considered. In the intravehicular detection phase, the technique relies on beacon message broadcast with TDMA technique. TDMA preserves the allocated time splitting timetable for the existing cluster of vehicles, in two-way message transmission from elected CHs to vehicle members in the network [9]. Packet Beacon messages received from the prior adjacent vehicle are checked before sending to the roadside unit (RSU) for position verification, message authentication and alerting analysis of the vehicle [10], [36].

This paper compares their proposed technique with other multihop networks such as P2DAP, SKC and EAPDA in terms of energy consumption, accuracy estimation of beacon message time synchronization and the probability of detection of Sybil attacks for connected vehicles at distributed VANETs environment. The results confirm that the proposed technique outperforms the exiting protocols over long transmission distance for Sybil attack detections in dynamic VANETs settings in terms of detection rate, measurement precision and energy efficiency.

The contribution of this paper can be summarized as follows:

- Spider monkey time synchronization (SMTS) was proposed for large-scale VANETs based on cooperative scenarios of CSMA/CA and TDMA detection time synchronization techniques.
- A bio-inspired spider monkey technique was employed as packet-controlled which is like an ant colony optimization that uses pheromone tracking technique for malicious nodes detection [33].
- Power consumption was investigated in randomly distributed packet beacon message to avoid message collisions and redundancy to maximize the network lifetime.
- Finally, the probability of detection for connected vehicles was evaluated and was compared to other detection protocols.

The remainder of this paper is organized as follows. In Section II, the related works are presented. Section III, presents analyzes of the network system model on how to detect the Sybil attacks two-way vehicle synchronization probability. Section IV presents the proposed techniques. In Section V, an estimation of the performances of the proposed technique by simulation was performed and Section VI concludes the proposed technique.

II. RELATED WORKS

Several harmonized biologically-inspired protocols for densely distributed large-scale sensor networks have been proposed. Castro *et al.* [6] proposed an autonomic biologically-inspired algorithm that enhanced routing efficiency in sensor networks. The nodes were assumed to be self-organized to broadcast beacon message among other cluster members.

Liu *et al.* [7] used bio-inspired QoS routing technique for mobile ad hoc networks to broadcast traffic data to nodes in the network preserving the security and privacy of data information against malicious node for secure communications. The security challenges in VANETs by consistent Sybil attack have attracted much attention in recent time due to their dynamic locations. Sybil vehicle attacker produces multiple false identities with wrong messages to harshly damage the standard functions of VANETs safety-associated applications. Yao *et al.* [11] proposed a new detection scheme for Sybil attack using voiceprint and received signal strength indicator (RSSI). To sidestep the wrong location estimation base on the threshold radio propagation reproductions in conventional RSSI detection systems, voiceprint uses the time series RSSI as vehicular speech and matches the likeness with received time series.

Schweitzer *et al.* [12] proposed a mean to detect the Sybil attack. Each node attack is being detected independently without help from VANET infrastructures, but this scheme highly relied on the collaboration among neighboring node to perform effective Sybil detection in the network. In [13], reduction of the gray-hole denial of service attack was investigated. The technique assumes no obvious node alliance, as various nodes depend on their routing information only. To protect VANETs from diverse attacks like distributed denial of service (DDoS) that aim at honest vehicles in the networks and the controllers from the source, the proposed technique must use different real time predefined security levels, whereas sustaining little overhead and minimal formation to avoid frequent vehicular attacks [14], [35].

Rabieh *et al.* [15] examined some security threats in identity-based batch verification scheme in the arbitrary oracle model, with little constant pairing number. The proposed scheme demonstrated a resilient performance in transmission overhead and delay computations without depending on the number of messages in honest vehicles to prevent impersonated vehicles from their privacy and stealing of private data. This preserved VANET data from the occurrence of identity falsification to improve network performance [16], [17]. The conventional VANET structures depend on detection algorithm at the occurrence of delay overhead to sense the risk at the verification time. An authentication key agreement model was proposed to authenticate from different vehicles multiple requests received. The model ignores priority request from emergency vehicles, allowing Sybil vehicle attack to falsify data and send the wrong message by swindling the identity of honest vehicles. To prevent this, Batch verifications algorithm based on priority is employed to mitigate time delay and checking early RSU timestamps to resist Sybil vehicle attacks on the honest vehicles [18]. To safeguard the VANET security protocol, a corporative mechanism for detecting malicious vehicles using the scalable and lightweight protocol to avoid

false detection and collusion attacks among honest vehicles. The honest vehicles use global positioning system to analyze the position of other honest vehicles by encrypting the privacy data from falsification by malicious vehicles [19], [34].

This protocol periodically sends protection connected messages with little computation overhead. Multitude identities produced malicious vehicles flood the network with the wrong message to cause Sybil vehicular attacks. Most researchers focus on conventional approach to preserve and validate data information. Few schemes are proposed for probability of detection of Sybil vehicles and frequent number of its attacks on legitimate vehicles in secure beacon message dissemination.

III. NETWORK SYSTEM MODEL
This section explains the model of the Spider monkey detection that was considered as shown in Figure 1. The Sybil attacking strategies, how to predict the number of Sybil attacks on VANETs, and detection of malicious nodes among the connected vehicles.

A. SPIDER MONKEY DETECTION MODEL
A meta-heuristic is gathering of algorithmic observations that are used to illustrate and determine the decision-making difficulties by offering satisfactory results [20]. Artificial spider is a packet-controlled similar to the insect with restricted memory but capable of performing assigned tasks. They navigate over fully connected formation graph G (V, E); where V designates set of sensor nodes and E specifies the communication links that mutually connects the vertices of sensor nodes. Artificial spiders route along vertices through the edges. In each vertex navigated, a fractional detection is attained by dropping certain quantity of pheromone and results are achieved in a step-by-step approach while monitoring the network through a correlated signal line, an idea compared with [14]. To realize the prospective node, fractional detections are estimated to allow local exploration to detect the sensor node at destination and consistent update of pheromone by each node along transmission distance to arrive the destination. To maintain reliable routing table as pheromone perishes for the optimal pathway selected, the initial fractional detection and pheromone rate among all adjacent nodes are given equal probability to respond o variations in the [21]–[23], [33]. Some terms used to describe the RSU behavior are clearly described below.

- *Vehicles:* The vehicles can communicate with RSUs and other vehicles as they are equipped global positioning systems (GPS) to authenticate the privacy key preservation to avoid data falsification. The vehicles receive constant pseudonyms information and periodically use trusted certificate authority to verify them before their deployment.
- Roadside unit (*RSU*): It is access points that are installed on the roads. They served as a medium of communication between the Department of Motor Vehicles (DMV), vehicles and other RSUs. They use directional
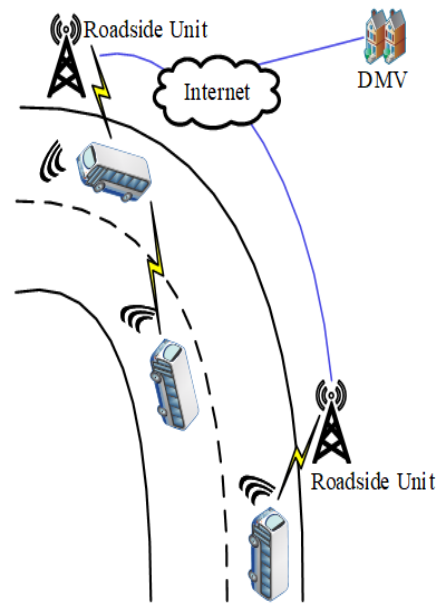

FIGURE 1. Network model illustration.

antennae to validate radio signals in detecting Sybil vehicles at narrow zones by broadcasting messages using the pseudonym identities to the DMV.

- *Department of Motor Vehicles (DMV):* They are in charge for deployment of RSUs, registration of vehicles for the security and safety of VANETs. The DMV has the authority to instruct the certificate authority to withdraw vehicle's permit when they detect potentiality of a vehicle to introduce Sybil attack.
- *Certificate of Authority (CA):* CA is mandated for providing and revoking digitally certified pseudonyms issued to vehicles when required. Vehicles periodically received the pseudonyms from CA during the vehicle registration and inspection.

B. SYBIL ATTACKING STRATEGIES
In vehicular networks, Sybil vehicle attack occurs as malicious node impersonates honest vehicles by demanding false identities. Mostly, Sybil attacker possibly will generate multiple additional vehicle identities randomly. The two probable extents in which a Sybil attack can function are:

1) COMMUNICATION INTERFERENCE
The Sybil attacker interrupts communication in two different approaches. For direct communication, the Sybil attack is for the Sybil vehicle to communicate with honest vehicles directly. As the honest vehicle broadcast radio message to a Sybil vehicle, malicious device intercept and listen to the message. Similarly, messages sent by Sybil vehicles are truly directed from the malicious devices instead. For indirect communication, the Sybil attacker and the honest vehicle communicate indirectly. Messages sent by Sybil vehicle are routed through malicious devices to another Sybil vehicle.

2) FICTITIOUS IDENTITIES

Sybil node produces new self-identity, creating multiple identifiers arbitrarily and purposely steals the identity of an honest vehicle. The stolen identity can go on undetected if the imitated vehicle is destroyed or momentarily restricted from the network. By limiting the array of honest identities through security mechanisms, it becomes worst in detecting the impersonating identities. However, the attacker allows its false identities take part in the network activities at once. They intercept useful data information and falsely act as honest vehicle simultaneously in a periodic manner to avoid being detected. In case of misbehavior detection in VANETs, an attacker with several Sybil nodes can easily spread the blame to confuse the system to sanction the misbehaved nodes to the Sybil attacker as shown in [24]. This leads to the Sybil attacker disturbing the reasonable resources allocation by passing on a resource severally to the same node and altering its identity.

C. PREDICTING THE NUMBER OF SYBIL ATTACKS ON VANETs

This paper assumes that the honest vehicle approaches roadways will have a higher risk of Sybil attacks as false information sent from Sybil vehicles impersonate identity. Therefore, the probability of vehicle collision, P occurring is defined as

$$P = N_a \times P_c \tag{1}$$

where N_a is the probability of collision when no aversive maneuvers made and P_c is the probability of failing to avoid Sybil attacks in the system.
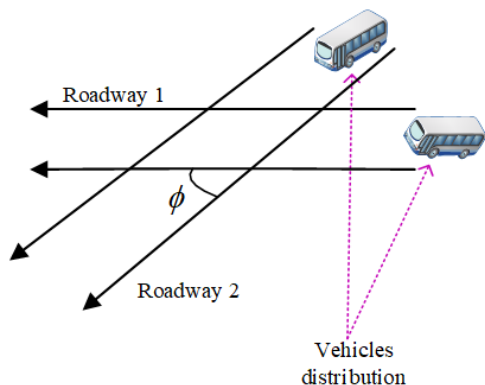

FIGURE 2. Vehicles crossing roadways.

In the proposed technique, the paper considers crossing of two highways model as demonstrated in Figure 2. The model establishes that there is probability of collision if Sybil vehicles succeed in truncating the information from reaching the destined vehicles. Two incoming vehicles reaching the crossing area are easily to collide. The vehicle in the roadway 1 approaches the vehicle in the roadway 2 with relative velocity given as

$$V_{ij} = \sqrt{\left(V_i^{(1)}\right)^2 + \left(V_j^{(2)}\right)^2 - 2V_i^{(1)}V_j^{(2)}\cos\phi} \tag{2}$$

where $V_i^{(1)}$ is the velocity of vehicle class i in roadway 1, $V_j^{(2)}$ is the velocity of vehicle class j in roadway 2 and the angle of direction between incoming vehicles is ϕ as illustrated in Figure 2.

The likelihood diameter of the collision becomes

$$D_{ij} = \frac{L_i^{(1)}V_j^{(2)} + L_j^{(2)}V_i^{(1)}}{V_{ij}}\sin\phi$$
$$+ B_j^{(2)}\left[1 - \left(\sin\phi\frac{V_i^{(1)}}{V_{ij}}\right)\right]^{1/2}$$
$$+ B_i^{(1)}\left[1 - \left(\sin\phi\frac{V_j^{(2)}}{V_{ij}}\right)\right]^{1/2} \tag{3}$$

where $L_i^{(1)}$ is the dimension of vehicle class i in the roadway 1, $L_j^{(2)}$ is the dimension of vehicle class j in the roadway 2 and B is the size of vehicle.

Therefore, the number of vehicle possible collision can be estimated by using

$$N_A = \sum_i \sum_j \iint \frac{Q_{1i}Q_{2j} + L_j^{(2)}V_i^{(1)}}{V_i^{(1)}V_j^2} f_i^{(1)}(Z)f_j^{(2)}V_{ij}D_{ij}dA\Delta t \tag{4}$$

where Q_{ij} are the number of vehicular movements at roadways in period time of Δt. Z_i is the covered distance from the intermediate point of the roadway 2 and f is the Gaussian distribution for lateral traffic distribute of vehicle in considered roadways expressed as

$$f_j^{(2)}(z_j) = \frac{1}{\sigma_j^{(2)}}\exp\left[\frac{-(z_j - \mu_i^{(2)})^2}{2(\sigma_j^{(2)})^2}\right] \tag{5}$$

where $\mu_i^{(2)}$ represents the mean quantity of z_j and $\sigma_j^{(2)}$ denotes the standard deviation of z_j. Therefore, the number of probability of vehicular collision can be achieved when (4) and (5) are multiplied [25].

D. DETECTION OF MALICIOUS VEHICLES AMONG CONNECTED LEGITIMATE VEHICLES

It was assumed that the honest vehicle periodically sends packet beacon message at a given time interval. This paper uses three approaches to detect the malicious nodes. These are:

1) POSITION VERIFICATION

As the network topology dynamically changes, there is no need to locate the position of the honest vehicles at the shortest possible time.

Individual vehicle occasionally transmits a packet beacon information format comprises of a pseudonym, position coordinates, timestamp and vehicular up-to-date speed to the intended vehicle. Authentication is done confidentially by the beacon to avoid revealing the vehicle private data information to suspected vehicles and malicious nodes.
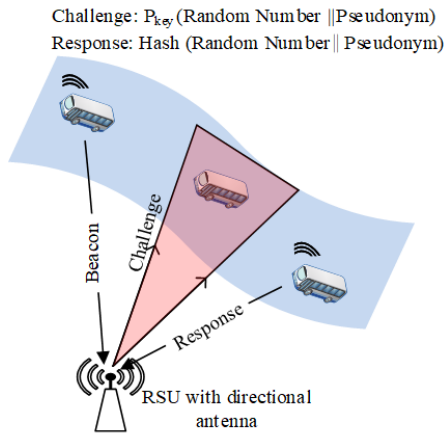
Challenge: P_{key} (Random Number $\parallel$ Pseudonym)
Response: Hash (Random Number $\parallel$ Pseudonym)

FIGURE 3. Challenge-response among vehicle and RSU.

From Figure 3, the public key encrypted vehicle by the challenge packet has a random number and the pseudonym. This implies that the RSU estimates the new position spread over the propagation delay and current vehicular speed of the beacon and the dissemination time taken by challenge packets to arrive the destination vehicles.

The RSU is equipped with a directional antenna that transmits both the random number and its pseudonym from the challenge packet to the vehicle to confirm their positions. RSU compares the random number pseudonym received from previous vehicles and if the hash values are identical, the falsified position is verified, else the vehicle is deemed as Sybil attacked vehicle [26]. Again, if no response is received after the timer expires; the RSU suspects the vehicle of falsifying its position and therefore send to DMV a pseudonym of the vehicle for more inquiry. When the case is proved to be true, the DMV faults the vehicle of Sybil attack and allows CA to withdraw its certificates to reduce the false alarming rate significantly.

Assume the beacon signal is successfully acknowledged by the honest vehicle, the probability to verify the position correctly can be expressed as

$$QP_0P + (1 - Q)P_1P. \qquad (6)$$

Where compound occurrence, QP_0P indicates particular vehicle that reaches the vulnerable zone at likely time interval and the response signal distributed correctly, and $(1 - Q)P_1P$ corresponds to compound occurrence with incorrect prediction. The operative reception of contest signal accepted by preoccupied signal separates the vulnerable zone and exact response signal delivery. The parameter P is the probability that beacon signal positively reaches the RSU from the honest vehicle. P_0 represents the probability of response signal positively acknowledged by a vehicle at vulnerable zone. P_1 is the probability that a susceptible signal is positively acknowledged by the legitimate vehicle outside the vulnerable zone. Q designates the probability that legitimate vehicle enters the vulnerable zone within the feasible time interval.

Since these two occurrences are exclusive mutually, the paper assumes the probability of false alarming rate, P_f as

$$
\begin{aligned}
P_f &= 1 - [QP_0P + P - PQP_1] \\
&= 1 - [QP_0 + (1 - Q)P_1]P \\
&\approx 1 - QP_0P \qquad (7)
\end{aligned}
$$

Thus, the probability of detection performed correctly on honest vehicle that transmits false position, P_d is given by

$$
\begin{aligned}
P_d &> \Pr(\psi_1)1 = P(1 - P_1) \qquad (8) \\
P_d &\leq \Pr(\psi_1) + \Pr(\psi_2) \\
&= P(1 - P_1) + PP_1(1 - P) \qquad (9)
\end{aligned}
$$

Taking $0 \approx P_1 \ll 1$ and $\Pr(\psi_2)$ as infinitesimal, the approximation bounded limit, P_d is given by

$$
\begin{aligned}
P_d &\approx P(1 - P_1) + [PP_1(1 - P)]/2 \\
&= P - [PP_1(1 - P)]/2 \qquad (10)
\end{aligned}
$$

The P_d and P_f can be determined if parameters P_0, P_1, P and Q are given. Table 1 illustrates three scenarios where false positions of malicious vehicles can be recognized. ψ_1 and ψ_2 correspond to the lower and upper bound of P_d [27], [28].

2) MESSAGE AUTHENTICATION
Beacon messages sent are authenticated to guarantee security during the packets delivery among the vehicles. An individual vehicle has unique Identification (ID) and sends beacon information in a complete format such as source ID, destination ID, message ID and packet ID, to synchronize the cluster vehicle time and that of sensor nodes together. Detection of malicious node is done by comparing the vehicle ID of broadcast and received beacon message [29], [30].

3) ALARMING ANALYSIS
To minimize the communication overhead, packet beacon message must be sent only when RSU suspects the presence of malicious vehicles to cause Sybil attack. RSU can detect Sybil attack using the following techniques to suspect anomalies in the intended vehicle.

Vehicles Count: RSU compares the beacon message received with the previous before forwarding it to the next RSU. If there are an increased number of vehicles received, RSU suspects the possible occurrence of Sybil attack [31].

Accessibility Verification: The attacker forges the locations of honest vehicle with multiple identities before it can launch an active attack. RSU calculates the magnitude between itself and the received beacon packet, and if the magnitude is found to exceed the maximum transmission distance of RSU, the Sybil attack is suspected.

Location Overlapping: RSU suspects all vehicles overlapping a certain location close to an honest vehicle as potential threat to fake location identities [32] and to launch the Sybil attack [32].

TABLE 1. Position verification analysis for connected vehicles at false positions.

Compound Occurrence	Beacon Signal	Vulnerable Signal	Response Signal	Position Verification
ψ_1	positively acknowledged	missed	-	authenticated
ψ_2	positively acknowledged	positively acknowledged (caused by signal rebound)	missed	authenticated
ψ_3	positively acknowledged	positively acknowledged (caused by signal rebound)	positively acknowledged	no authenticate

IV. PROPOSED TECHNIQUES

This section explains in detail the Spider Monkey Detection Technique, Spider Inter-Vehicle Time Synchronization Technique and Spider Intra-Vehicle Time Synchronization Technique

A. SPIDER MONKEY DETECTION TECHNIQUE

The proposed technique is based on the meta-heuristic stimulated framework process by natural spider monkey behavior. Artificial Spider Monkey was used numerically to detect the malicious nodes that caused the Sybil attacks on the honest VANETs. TDMA approach was used to split timeslots during the mobility of the node to synchronize with neighboring nodes with different timeslots. When an autonomous decentralized local detection synchronization was employed as non-deterministic communication delays, a less packet beacon message transmission interferences was formed with variation in local alarm pheromone clocks and random initial clock offsets.

The cluster honest vehicles elected one vehicle as the cluster head (CH) for the nodes within the data transmission distance and other vehicles periodically announce their presence by broadcasting the available packet beacon messages. The vehicles are equipped with alarm pheromone secreted to monitor the sensor nodes and detect malicious nodes intrusion as it compares beacon message dissemination time from the source vehicle to time packet information and received at the destination to check clock offset and propagation delay to detect the Sybil attack. The proposed technique performances were compared for distributed large-scale VANETs in a two-way message dissemination method.

B. SPIDER INTER-VEHICLE DETECTION TIME SYNCHRONIZATION TECHNIQUE

As packet information being transmitted, the sensor nodes pathway is guaranteed positively in pheromone secreted quantity. A pairwise technique was assumed to transmit beacon message among the vehicles in the network. The source vehicle sends *Sync_start*, at the preliminary stage by the sensor node in adjacent CH selected to the base station (BS).
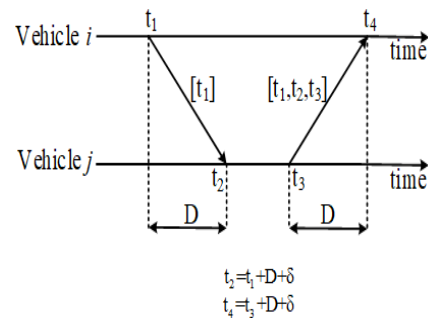

FIGURE 4. Two-way vehicular communication model.

As BS receives *Sync_start* message, it then retransmits beacon message *Sync_req* at waiting time randomly with broadcast initial time t_1. Discretely, vehicle keeps a *Sync_table*, to maintain neighboring vehicles record moving in the same pathway, as demonstrated in the Figure 4. It is established in Figure 4 that vehicle *j* sends an acknowledgement (ACK) to the broadcasted message at time t_3, considering timestamps t_1, t_2 and t_3. On time t_4, subsequent message is acknowledged by both vehicles to adjust the clock offset. Therefore, the vehicle *i* accurately estimates propagation delay, P_{delay} as

$$P_{delay} = \frac{[(t_2 - t_1) + (t_4 - t_3)]}{2} \quad (11)$$

Additionally, the clock offset, C_{offset} of vehicle *i* is found as

$$C_{offset} = \frac{[(t_2 - t_1) - (t_4 - t_3)]}{2} \quad (12)$$

It is observed that propagation delay remains constant in both directions and clock drift is constant between the corresponding dimensions at the assigned time. The accepted vehicle *i* message determines the clock offset cost to synchronize with vehicle *j*. This guarantees that, the clock of vehicle *i*, can be correctly detected by vehicle *j* in tracking the malicious vehicles to avoid Sybil attacks as in Algorithm 1.

C. SPIDER INTRA-VEHICLE DETECTION TIME SYNCHRONIZATION TECHNIQUE

This subsection assumes reference broadcast method to send beacon messages amongst CH and vehicle members.

Algorithm 1 Intervehicle Time Synchronization

BS Station:
    broadcast (Sync_start, level = 0);
    if receive(Sync_rec) then
    send (Sync_ack, t_1, t_2, t_3);
  Neighbor honest vehicles:
    receive (Sync_start, level)
    if (level = null) then
    {
        level++;
        wait a short random time;
        send(Sync_req,level, t_1);
        receive(Sync_ack);
        {
            record (t_1, t_2, t_3, t_4);
         calculate (P_{delay}, C_{offset});
         Sync (P_{delay}, C_{offset});
        }
    }
  else end message;

The proposed technique operates within transmission range as vehicle *i* sends beacon message to vehicle *j* for starting synchronization process.

Let the timestamps in vehicle *i* and vehicle *j* be T_i and T_j accordingly in receiving *i*th cooperative beacon message. The maximum likelihood (ML) for clock offset is calculated the between vehicle *i* and vehicle*j* as

$$ML_{ij} = \frac{1}{L} \sum_{i=1}^{L} [T_i - T_j] \qquad (13)$$

where *L* indicates the total quantity of cooperative beacon messages communicated between vehicle *i* and vehicle *j*.

The proposed technique at the access and broadcast time can eliminate non-deterministic errors along the transmission distance. This is done to provide improvement for synchronization accuracy between vehicles to maximize energy efficiency to prolong network lifetime.

V. NUMERICAL AND SIMULATION RESULTS

This section evaluates the proposed technique as a meta-heuristic stimulated framework process by natural spider monkey behavior using numerical simulation. The following assumptions were made in the simulation that the sensor nodes are randomly distributed at transmission distance in an area of 160×160. Each sensor node has unique vehicle ID equipped with GPS for the collective time to form cluster. At the initial detection stage, it is assumed that the CH and the nodes successfully broadcast beacon message to connected legitimate vehicles.

In the proposed technique, the paper investigates closeness of malicious vehicles. Detection limits are set with secreted pheromone value in alerting the legitimate vehicles of an impending Sybil attacks. 90%, 95% and 98% were used as

detection limits for detecting the malicious vehicles with multiple identities as shown in Figure 5 and Figure 6.
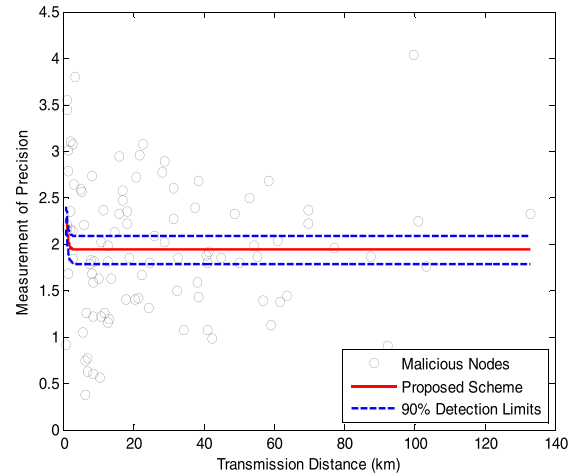
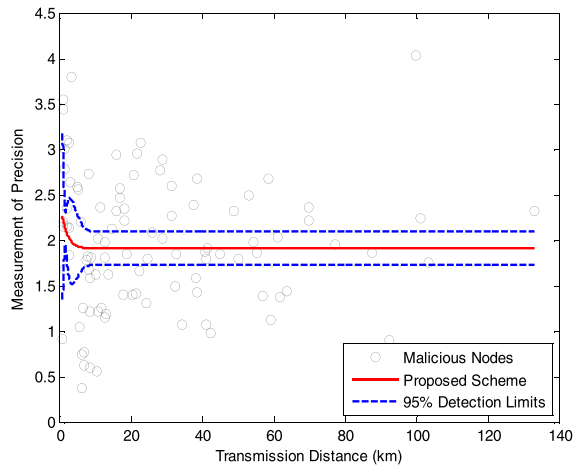**FIGURE 5.** Measurement of precision at detection limit 90%.

FIGURE 6. Measurement of precision at detection limit 95%.

The principal functions of detection limit are to monitor connected legitimate vehicle' activities and the network performance at different layers. The precision of Sybil attack detection is largely measured in terms of false alarming and false detection. Therefore, the proposed technique measures precision by observing number of legitimate vehicles at optimal confidence intervals. With a positive increase in pheromone value in the measurement of precision of connected legitimate vehicles, the transmission distance increases steadily with different detection limits. However, the higher the detection limits, the better the detection. Thus, 98% detection limit will outperform other detection limits as shown in Figure 7.

At low secreted pheromone quantity with the transmission distance increases, the probability of detection declines as illustrated in Figure 8. The throughput decreases due to equal level interference to decrease energy efficiency for the total network. As probability of detection decreases, SMTS detects
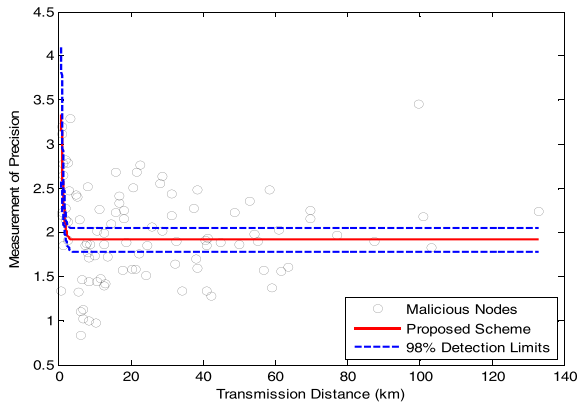
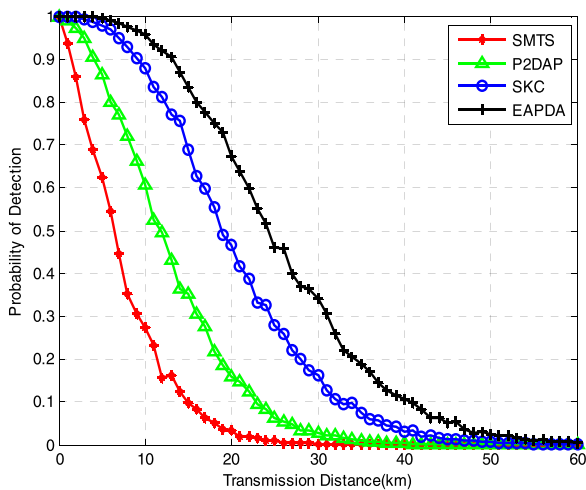**FIGURE 7.** Measurement of precision at detection limit 98%.
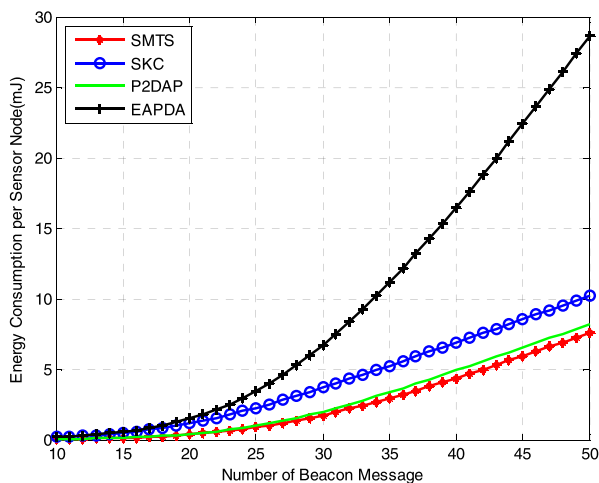

FIGURE 8. Transmission distance.

FIGURE 9. Energy consumption.

the potential malicious vehicles better. This avoids the malicious vehicle to launch attack on legitimate vehicles at the densely deployed region than other protocols. Figure 9 illustrates total energy consumption of network with different number of protocols. At high positive secreted pheromone value. It is observed that at high energy consumption, the

interference of beacon messages dissemination varies. Probability of false alarming and collision occurrence increases among closed vehicles. SMTS performs better than P2DAP, SKC and EAPDA protocols as they have higher power consumption rate.

VI. CONCLUSION

This paper proposed a novel biologically-inspired spider monkey time synchronization (SMTS) techniques for large-scale VANETs. The proposed technique was based on the meta-heuristic inspired performance by natural spider monkey behavior. The technique uses an artificial spider monkey to detect the malicious nodes that causes Sybil attacks on honest vehicles and reduces packet beacon message loss, clock offset and propagation delay at densely deployed challenge zone to minimize energy consumption in the total network topology. The network was split into intervehicle detection time clustering synchronization level as connected vehicles (assumed two-way message packet beacon message exchange technique) to harmonize the BS clock and that of CHs to create hierarchical topology structure. Again, in the intra-vehicle detection time synchronization level, the reference broadcast technique is assumed in detecting time synchronization among the connected vehicle members and the elected CHs. The results obtained validate that the proposed technique outperforms the existing protocols over long transmission distance for Sybil attack detections in dynamic VANETs settings in terms of detection rate, measurement precision and energy efficiency.

REFERENCES

[1] Y. Toor, P. Muhlethaler, and A. Laouiti, "Vehicle ad hoc networks: Applications and related technical issues," *IEEE Commun. Surveys Tuts.*, vol. 10, no. 3, pp. 74–88, 3rd Quart., 2008.

[2] Y. Bi, L. X. Cai, X. Shen, and H. Zhao, "Efficient and reliable broadcast in intervehicle communication networks: A cross-layer approach," *IEEE Trans. Veh. Technol.*, vol. 59, no. 5, pp. 2404–2417, Jun. 2010.

[3] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "P2DAP—Sybil attacks detection in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 582–594, Mar. 2011.

[4] D. S. Reddy, V. Bapuji, A. Govardhan, and S. V. N. Sarma, "Sybil attack detection technique using session key certificate in vehicular ad hoc networks," in *Proc. IEEE Int. Conf. Algorithms, Methodol., Models Appl. Emerg. Technol. (ICAMMAET)*, Feb. 2017, pp. 1–5.

[5] A. Singh and P. Sharma, "A novel mechanism for detecting DOS attack in VANET using enhanced attacked packet detection algorithm (EAPDA)," in *Proc. IEEE 2nd Int. Conf. Recent Adv. Eng. Comput. Sci. (RAECS)*, Dec. 2015, pp. 1–5.

[6] M. F. de Castro, L. B. Ribeiro, and C. H. S. Oliveira, "An autonomic bio-inspired algorithm for wireless sensor network self-organization and efficient routing," *J. Netw. Comput. Appl.*, vol. 35, no. 6, pp. 2003–2015, 2012.

[7] Z. Liu, M. Z. Kwiatkowska, and C. Constantinou, "A biologically inspired QoS routing algorithm for mobile ad hoc networks," *Int. J. Wireless Mobile Comput.*, vol. 4, no. 2, pp. 64–75, 2010.

[8] J. Li, W. Zeng, and A. Arora, "Chameleon: On the energy efficiency of exploiting multiple frequencies in wireless sensor networks," in *Proc. Int. Conf. Broadband Commun., Netw. Syst.*, 2012, pp. 138–157.

[9] V. Nguyen *et al.*, "An efficient time slot acquisition on the hybrid TDMA/CSMA multichannel MAC in VANETs," *IEEE Commun. Lett.*, vol. 20, no. 5, pp. 970–973, May 2016.

[10] C. Chen, X. Wang, W. Han, and B. Zang, "A robust detection of the sybil attack in urban VANETs," in *Proc. IEEE Int. Conf. 29th Distrib. Comput. Syst. Workshops*, Jun. 2009, pp. 270–276.

[11] Y. Yao *et al.*, "Voiceprint: A novel Sybil attack detection method based on RSSI for VANETs," in *Proc. IEEE/IFIP Int. Conf. Dependable Syst. Netw. (DSN)*, Jun. 2017, pp. 591–602.

[12] N. Schweitzer, A. Stulman, R. D. Margalit, and A. Shabtai, "Contradiction based gray-hole attack minimization for ad-hoc networks," *IEEE Trans. Mobile Comput.*, vol. 16, no. 8, pp. 2174–2183, Aug. 2017.

[13] A. Hussein, I. H. Elhajj, A. Chehab, and A. Kayssi, "SDN VANETs in 5G: An architecture for resilient security services," in *Proc. IEEE 4th Int. Conf. Softw. Defined Syst. (SDS)*, May 2017, pp. 67–74.

[14] M. Shafiq, X. Yu, A. K. Bashir, H. N. Chaudhry, and D. A. Wang, "A machine learning approach for feature selection traffic classification using security analysis," *J. Supercomput.*, Jan. 2018, doi: 10.1007/s11227-018-2263-3.

[15] K. Rabieh, M. M. E. A. Mahmoud, and M. Younis, "Privacy-preserving route reporting schemes for traffic management systems," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2703–2713, Mar. 2017.

[16] D. B. Rawat, B. B. Bista, and G. Yan, "Securing vehicular ad-hoc networks from data falsification attacks," in *Proc. IEEE Region 10 Conf. (TENCON)*, Nov. 2016, pp. 99–102.

[17] Y. Hao, J. Tang, and Y. Cheng, "Cooperative sybil attack detection for position based applications in privacy preserved VANETs," in *Proc. IEEE Global Telecommun. Conf. (GLOBECOM)*, Dec. 2011, pp. 1–5.

[18] Y. Y. Nasrallah, I. Al-Anbagi, and H. T. Mouftah, "Distributed time synchronization mechanism for large-scale vehicular networks," in *Proc. IEEE Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Apr. 2016, pp. 1–6.

[19] D. Shukla, A. Vaibhav, S. Das, and P. Johri, "Security and attack analysis for vehicular ad hoc network—A survey," in *Proc. IEEE Int. Conf. Comput., Commun. Automat. (ICCCA)*, Apr. 2016, pp. 625–630.

[20] S. Archana and N. P. Saravanan, "Biologically inspired QoS aware routing protocol to optimize lifetime in sensor networks," in *Proc. IEEE Int. Conf. Recent Trends Inf. Technol.*, Apr. 2014, pp. 1–6.

[21] H. Byun, S. Son, and S. Yang, "Biologically inspired node scheduling control for wireless sensor networks," *J. Commun. Netw.*, vol. 17, no. 5, pp. 506–516, 2015.

[22] D. Tian *et al.*, "A microbial inspired routing protocol for VANETs," *IEEE J. Internet Things*, vol. 5, no. 4, pp. 2293–2303, Aug. 2018.

[23] B. Yu, C.-Z. Xu, and B. Xiao, "Detecting Sybil attacks in VANETs," *J. Parallel Distrib. Comput.*, vol. 73, no. 6, pp. 746–756, 2013.

[24] G. Yan, W. Yang, J. Lin, and D. B. Rawat, "Cross-layer location information security in vehicular networks," *J. Next Gener. Inf. Technol.*, vol. 3, no. 2, pp. 37–56, 2012.

[25] P. T. Pedersen, "Collision and grounding mechanics," in *Proc. WEMT*, 1995, pp. 125–157.

[26] M. Abu-Elkheir, S. A. Hamid, H. S. Hassanein, I. B. M. Elhenawy, and S. Elmougy, "Position verification for vehicular networks via analyzing two-hop neighbors information," in *Proc. IEEE 36th Conf. Local Comput. Netw. (LCN)*, Oct. 2011, pp. 805–812.

[27] K. Rabieh, M. M. E. A. Mahmoud, T. N. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding Sybil attack in VANETs," in *Proc. IEEEb Commun. Inf. Syst. Secur. Symp. (ICC)*, Jun. 2015, pp. 7298–7303.

[28] M. H. DeGroot and M. J. Schervish, *Probability and Statistics*, 4th ed. London, U.K.: Pearson, 2010.

[29] S. Wang, A. Pervez, and M. Nekovee, "Converging time synchronization algorithm for highly dynamic vehicular ad hoc networks (VANETs)," in *Proc. IEEE 7th Int. Symp. Commun. Syst., Netw. Digit. Signal Process. (CSNDSP)*, Jul. 2010, pp. 443–448.

[30] S. B. M. Baskaran, G. Raja, A. K. Bashir, and M. Murata, "QoS-aware frequency-based 4G+relative authentication model for next generation LTE and its dependent public safety networks," *IEEE Access*, vol. 5, pp. 21977–21991, 2017.

[31] S. Yaseen *et al.*, "Improved generalization for secure data publishing," *IEEE Access*, vol. 6, pp. 27156–27165, 2018.

[32] R. Arul, G. Raja, A. K. Bashir, J. A. Chaudry, and A. Ali, "A console GRID leveraged authentication and key agreement mechanism for LTE/SAE," *IEEE Trans. Ind. Informat.*, vol. 14, no. 6, pp. 2677–2689, Jun. 2018.

[33] C. Iwendi, Z. Zhang, and X. Du, "ACO based key management routing mechanism for WSN security and data collection," in *Proc. 19th IEEE Int. Conf. Ind. Technol.*, Feb. 2018, pp. 1935–1939.

[34] I. Yaqoob *et al.*, "The rise of ransomware and emerging security challenges in the Internet of Things," *Comput. Netw.*, vol. 129, pp. 444–458, Dec. 2017.

[35] R. Kolandaisamy *et al.*, "A multivariant stream analysis approach to detect and mitigate DDoS attacks in vehicular ad hoc networks," *Wireless Commun. Mobile Comput.*, vol. 2018, May 2018, Art. no. 2874509, doi: /10.1155/2018/2874509.

[36] S. A. Hussain *et al.*, "An efficient channel access scheme for vehicular ad hoc networks," *Mobile Inf. Syst.*, vol. 2017, Jun. 2017, Art. no. 8246050, doi: 10.1155/2017/8246050.

CELESTINE IWENDI (SM'17) received the second master's degree in communication hardware and microsystem engineering from Uppsala University, Sweden, in 2008, ranking under 100 in the world University ranking, and the Ph.D. degree in electronics from the University of Aberdeen, U.K., in 2013. He is currently an Associate Professor with the Bangor College China, Central South University of Forestry and Technology, Hunan, China.

He is a highly motivated researcher with the book *Wireless Sensor Network Security* and over 100 publications. He is currently a Senior Lecturer with the Bangor College China and has a strong teaching emphasis on communication, has hands-on experience, is willing to learn, and is an 18-year technical expertise, and currently teaches the Engineering Team Project, Circuit Theory, Data Networks and Distributed Systems, and Control Systems. He has developed operational, maintenance, and testing procedures for electronic products, components, equipment, and systems; and provided technical support and instruction to staff and customers.

He is a Wireless Sensor Network Chief Evangelist, a researcher, and a designer. His research focuses on wireless sensor networks, Security of Things, communication controls, Internet of Things (IoT), electromagnetic machines, 5G networks, and low-power communication protocols. He has been a Board Member of the IEEE Sweden Section since 2017and is an Associate Fellow of the Higher Education Academy, U.K., to add to his teaching and professional experiences. He is the Co-Chair of the special session on Wireless Sensor Networks: Hardware/Software Design Aspects for Industry at the Prestigious International Conference of Industrial Technology ICIT. He is an Editor of the *International Journal of Engineering and Allied Disciplines* in 2015, a Newsletter Editor of the IEEE Sweden Section from 2016 to 2018, the Editor-in-Chief of the *Wireless Sensor Network Magazine* in 2009, a Committee Member of the International Advisory Panel and the International Conference on Marine, Ocean and Environmental Sciences and Technologies from 2014 to 2016, the Editor-in-Chief of the *Journal of Wireless Sensor Network* in 2009, the Advisory Board, and the *International Journal of Innovative Computer Science and Engineering* 2013.

MUEEN UDDIN received the B.S. and M.S. degrees in computer science from Isra University, Pakistan, with a major in computer networks and security, and the Ph.D. degree from Universiti Teknologi Malaysia in 2013, with focus on energy-efficient cloud data centers. He is currently with the Department of Information System, Effat University, Jeddah, Saudi Arabia, as an Assistant Professor. He has authored over 80 international journal papers published in various highly indexed and reputed journals with a cumulative impact factor over 35. His research interests include green computing infrastructures, energy-efficient cloud data centers, network security, MANET routing protocols, virtualizations, and renewable energy.

JAMES A. ANSERE received the B.Sc. degree in physics from the University of Cape Coast, Ghana, in 2007, and the M.Sc. degree in telecommunication engineering from the Blekinge Institute of Technology, Sweden, in 2012. He was a Lecturer with Sunyani Technical University. He has authored over 12 international papers. He is a peer reviewer for the International Telecommunication System.

He is currently pursuing the Ph.D. degree with the College of Internet of Things Engineering, Hohai University, China. His research interests are 5G wireless networks, Internet of Things, massive MIMO, and wireless and mobile communications. He wa s a recipient of the Sparbanksstiftelsen Kronan Award for the master's Thesis, in 2012, and the Fellowship Award from the Civilian Institute of Democratic Administration, West Africa, in 2017.

P. NKURUNZIZA received the B.Sc. degree in electronics and communication systems engineering from the College of Science and Technology, University of Rwanda, Rwanda, in 2014. He is currently pursuing the master's degree in information and communication engineering with the College of Internet of Things Engineering, Hohai University, China. His current research interests include cellular wireless communications, massive MIMO technology, and 5G cellular networks.

J. H. ANAJEMBA received the M.Sc. degree in information communication technology from the National Open University of Nigeria in 2016. He is currently pursuing the Ph.D. degree in information and communication engineering with the College of Internet of Things Engineering, Hohai University, China. His current research interests include cellular wireless communications, antenna and V2V technology, and 5G cellular networks and security.

ALI KASHIF BASHIR (M'15–SM'16) received the Ph.D. degree in computer science and engineering from Korea University, South Korea. He was with Osaka University, Japan; the Nara National College of Technology, Japan; the National Fusion Research Institute, South Korea; Southern Power Company Ltd., South Korea; and Seoul Metropolitan Government, South Korea. He is currently an Associate Professor with the Faculty of Science and Technology, University of the Faroe Islands, Tórshavn, Denmark. He is also with the Advanced Network Architecture Laboratory as a Joint Researcher. He is supervising/co-supervising several graduates (M.S. and Ph.D. students). His research interests include cloud computing, NFV/SDN, network virtualization, network security, IoT, computer networks, RFID, sensor networks, wireless networks, and distributed computing. He is the Chair of several conference sessions, gave several invited and keynote talks, and reviewed the technology leading articles for journals, such as the IEEE Transactions on Industrial Informatics, the *IEEE Communication Magazine*, the IEEE communication Letters, the IEEE Internet of Things, the IEICE journals, and conferences, such as the IEEE Infocom, the IEEE ICC, the IEEE Globecom, and the IEEE Cloud of Things. He is serving as the Editor-in-Chief for the IEEE Internet Technology Policy Newsletter and the IEEE Future Directions Newsletter. He has also served/serving as the guest editor on several special issues in the journals of the IEEE, Elsevier, and Springer. He is an Editorial Board Member of journals, such as the IEEE Access and the *Journal of Sensor Networks and the Data Communications*. He is actively involved in organizing workshops and conferences.

● ● ●