Global Journals LaTeX JournalKaleidoscope™
Artificial Intelligence formulated this projection for compatibility purposes from the original article published at Global Journals. However, this technology is currently in beta. *Therefore, kindly ignore odd layouts, missed formulae, text, tables, or figures.*

An Efficient Black-Hole and Worm-Hole Attacks Resilient Scheme for Cloud and Fog-Assisted Internet of Vehicles

Oladayo O. Olakanmi[1], Mbadiwe S. Benyeogor[2] and Kehinde O. Odeyemi[3]

[1] University of Ibadan

Received: 21 March 2021 Accepted: 10 April 2021 Published: 22 April 2021

Abstract

The Internet of Vehicles (IoV) is a distributed network that supports the use of data created by connected cars and vehicular ad-hoc networks (VANETs) for real-time communication among the vehicles and other infrastructures in the network. Although, IoV increases safety and efficient information exchange in transportation, its inter-connectivity exposes the vehicles and the people to different cyber-attacks such as black-hole and worm-hole which are capable of disrupting the network. In this paper, we identify the black-hole and worm-hole attacks as the major security threats to the IoV technology. We then propose periodic-time slicing and trust factor approaches to detect and prevent a black-hole attack and a cryptography procedure to prevent other IoV related cyber-attacks.

Index terms— car connectivity, cyber-security, cloud and fogassisted, internet of things, autonomous vehicles.

1 I. Introduction

s IoV becomes more connected and more autonomous with advanced communication technologies for robust transportation services, it also becomes more attractive and susceptible to different cyber-attacks. IoV faces various types of attacks, such as replay, eavesdropping, Sybil, blackhole, and worm-hole attacks, which result in security and privacy challenges in IoV. Of all these attacks, worm-hole and black-hole attacks are the most active and elusive to most existing security schemes. They easily degrade the performance and reliability of the IoV as a result of the dynamism of the IoV network. Several solutions based on watchdog, statistical, predictive, heuristic, timing, trust, and incentives-based approaches have been developed to prevent black-hole and worm-hole attacks in the vehicular ad-hoc network and IoV [5]. However, the high complexity, high delay, and non-adaptiveness of some of them make them unsuitable to IoV networks.

Asides from blackhole and wormhole attacks, enforcing privacy and data integrity are also the major issues in IoV. For example, malicious information from IoV can easily lead to loss of lives or compromise the privacy of the car and passenger. In consequence of these, there is a need for a security scheme not only resilient to worm-hole and blackhole attacks but also capable of guarantee the privacy and integrity of IoV data.

In this paper, we propose a security scheme for IoV capable of detecting black-hole and worm-hole attacks. It uses periodic-slices and their corresponding concatenated hash, sent to the destination node through the secondary nodes, to detect black-hole attacks and a cryptography-based procedure to detect worm-hole attacks. The scheme includes incentive and trust models to establish a reputation-based communication to encourage cooperation and reduce black-hole attacks in the IoV. A provable one message authentication code, using onetime and mutual keys, is used to affirm the data integrity. The contributions of this paper are as follows: 1. A non-complex periodic-slices approach to detect blackhole attacks and a cryptography-based procedure to detect worm-hole attacks. 2. Incentive and trust model to enforce reputation and cooperation in IoV. attacks.

The paper is organized thus; the related past works on the security issues on IoV and existing solutions are discussed in section 2. Section 3 is the system overview where we describe the primitive, system, and adversary model. Section 4 describes the methodology of the proposed scheme with its incentive and trust model. Section

5 involves performance evaluation, this section consists of the results of the experimental analysis. We concluded the work in Section 6.

2 II. Related Work

Detection and prevention of black-hole and worm-hole attacks are critical routing security issues in IoV. They can easily convert reliable cyber-physical paths in IoV for data and control packets routing into a compromised one. Meanwhile, they are elusive to most of the existing security solutions, therefore, the performance of IoV can be improved by making it resistible to malicious attacks likes black-hole and wormhole.

Black-hole attacker drops all packets it is supposed to forward to the destination node, meanwhile the worm-hole attacker re-direct packets taken from one location of the network to another part of the network.

Several approaches have been proposed to thwart blackhole in network [2], [8], [9], [10], [11], [3], [6], [12], [7]. For example, the work of Yao et al. [2] focus on blackhole. In the work, an entity-centric trust model is developed for detecting black-hole attacks, however, their approach may unfairly label honest nodes as black-hole attackers. Also, Daeinabi et al. [8] proposed an algorithm with a trust model capable of monitoring activities of a new entrant in VANET. The algorithm decreases the trust of a malicious new entrant who is dropping the packet and blacklists it once its trust is lower than the preset threshold. The authors in [9] improves the algorithm in [8] by enhancing the selection of the verifier and adding the prevention and isolation mechanism of blackhole attacks. Similar to [9], Uzma et al [10] enhanced the detection mechanism in [8] by increasing the verifier's selection criteria. In [11], Yao et al. developed a three-parameter of trust detection scheme for detecting selfish nodes in VANET.

Aside from using the trust model, the watchdog approach can still be used to detect black-hole. Watchdog approach checks the forwarding state of the forwarded packets by monitoring the next-hop neighbor can be used to thwart blackhole attack [3]. Hortelano et al. [6] adopted a watchdog and trust mechanism to detect a black-hole attack. Also, [12], adopted a watchdog technique to detect black-hole attacks.

Meanwhile, Delkesh et al. [7], proposed a heuristic approach for detecting black-hole attacks in mobile ad-oc networks. Their technique sends forged packets in the ad-hoc on-demand distance vector route discovery. Any node that replies to such fake destination IP address packets request is termed as a black-hole attacker. A predictive technique was used in [?] to prevent and detect intrusion. The approach can detect multiple misbehaviors of vehicles and selects the vehicle with the best trust value as the cluster head.

Like the black-hole, various solutions have also been proposed to detect worm-hole attacks in the network. Examples are the work in [15], [17], [18] and [16]. Safi et al. [15] introduced a solution that relies on the packet's maximum and allowed transmission distance in control packet and message authenticated packet [16] to detect worm-hole attacks. Hu et al. [17] adopted the temporal packet leash concept, with the notion of global clock synchronization. Their approach detects the worm-hole attacks from the exceptions in the packet transmission latency. C? apkun et al. [18] used round trip travel time for the packet delivery to detect unusual wormhole channels. However, [17] and [18] solution are hardware based and presence of a global clock.

3 III. Security Goals and Primitives

The security goals include detection of wormhole attacks, integrity, and black-hole attacks in the IoV. Also, we gear the scheme towards secure local and global access of IoV data. To achieve the security goals, we develop periodic-slices and non-complex cryptography approaches for thwarting the elusive attacks in IoV networks.

4 b) Primitives

We adopted a cyclic addition group G of order q and generator P, a cryptographic hash functions H : 0; 1* , , and a bilinear pairing e such that e : GXG G where l is the size of the secret key.

Table **??** shows the definition of the notations and symbols used in the scheme.

5 IV. Black-hole Resilient Scheme with Trust Factor

As shown in Figure **??**, the system model of the IoV scheme consists of entities such as vehicles, pedestrians, infrastructures, roadside units (RSU), and storage facilities, which include location-bound edge? ? Z * q , l H : 0, 1 * X0, 1 l ? Z * q a) Security Goals

and cloud server. Each entity can perform multi-hop communication such as vehicle to vehicle, vehicle to infrastructure, and vehicle to pedestrian. Each entity and the nearby edge generates a mutual public parameter and mutual secret key. The source entity, through either single-hop or multi-hop communication, pushes its IoV information to the destination. The destination verifies the instance of attack and computes a reputation-based incentive for the source. It uploads the IoV information to the edge for local access. The edge updates the source entity trust factor, reencrypts the IoV information with the source trust factor, and pushes it to the cloud server for global access. The cloud then decrypts the IoV information and updates its global trust table. The cloud re-encrypts the IoV information and the source trust factor with the edge's mutual secret keys and pushes it to the corresponding edges to complete a global-request.

The proposed scheme is divided into four phases; set-up and key management, IoV information hopping, IoV attacks detection and integrity test, incentive and trust factor generation phases, each of these phases are described below.

To set-up, each entity, cloud, and the nearby edge performs the following:

1. Each entity randomly generates while the edge and cloud generate kj and , respectively. Each entity computes and publishes its mutual public parameter as , while the edge j also computes and publishes its mutual public parameter as to the surrounding entity, who uses it to compute edgeentity mutual secret key as 2. Each entity then computes one-time-key as = , where and pseudonym as 3. The cloud randomly generates , computes and publishes it to the surrounding edges, who also uses it to compute edge-cloud mutual key as

6 b) IoV Data Hopping

For each hopping session, the source subdivides the unique session period into periods, selects the primary neighboring node for the IoV packet, and another secondary nodes for the transmission of the periodic slices and their concatenated hash value as shown in Figure **??**. It then sends the periodic slices and concatenated hash value to the destination through the secondary neighboring entities.

It sends one of the periodic-slices, encrypted packet, and message authentication code through the primary neighboring node to the destination.

The destination detects black-hole by recomputing the concatenated hash value, compare it with the received hash value. If equal, it indicates no black-hole attack otherwise black-hole is detected. In case there is no black-hole attack, the destination confirms the worm-hole attack through the received pseudonym and the data integrity. The destination then computes the incentive for the source node, uploads the copies of the encrypted IoV information and the incentive to the edge who updates the source trust factor. This phase is summarized as follows: 1. The source generates periodic-slices ; ::; t by sub-dividing the time stamp t into 2. The source selects the primary neighbouring entity for the IoV information m and another secondary entities within the coverage for the transmission of the periodic slices and hash value and encrypted source pseudonym as shown in Figure **??** and 3. 3. The source sends periodic slices and to the destination through the corresponding secondary neighbouring n entities. 4. Generates mutual key between the destination d and the source i as . Then, encrypted packet , encrypts pseudonym of the source as using one of the next unused one-timekey in its key chain, generates message authentication code , and sends through the primary neighbouring entity to the destination node.

7 c) IoV Attacks Detection and Integrity Test

As shown in Figures **??** and 3, to detect blackhole attack the destination on receiving IoV data ; c , and) from the primary entity and ; ::; t from secondary entities, it re-computes = H

. Checks , if holds, it implies no black-hole, otherwise black-hole is detected and drops the whole IoV information.

To detect worm-hole attack, the destination performs the following:

? Extracts and sends it to its edge for verification, who re-computes the edge-entity mutual key as ? The edge then re-computes the source one time secret key chain as = = 0; 1; ::;w, where = H). It decrypts the and for each checks if . If this does not hold for any of the then worm-hole attack detected otherwise the edge clears the source node of the worm-hole.

After receiving the worm-hole clearance from the edge, the destination checks the integrity of the data as follows:r * i ? Z * u *

? i = e(P, P) ri ? j = e(P, P) kj ? i ?j = ? rj j = e(P, P) rj ri . ? Re-computes the one-time-key, using the mutual public parameter of the source, as =? h+1 = 0 , 1, .., w H ?i ?j (? h) ?h ? 0 = H ?i ?j (? i ?j || i) i = H id i . ? c = e(P, P) u u * ? c ?j ? j ? c = ? kj c = e(P, P) urj . n n = n n ? 1 n t 1 , t 2 n ?1 , t n n . n = n n ?1 ? t = H(t 1 ||t 2 |..||t n) t 1 , t 2 , .., t n ?1 ? t ||? i ? i ?d = (? d) ri c i,t = E ? i ?d (m i,t) ? i = E ? h (i) ? = H ? i ?d (m i,t) t n , ?, ? i , c i,t (t n , ?, i ? i,t ? t t 1 , t 2 n ?1 , ? t n ? t (t 1 ||t 2 |..||t n) ? t ? = ? t ? i , ? i ? i ?j = ? i k j .. ? h+1 H ? i ?j (? h) ?h ? 0 ? i ?j ? j i (i = E ? i ?j ? i ? h+1 i ? = i ? h+1 a)

? Decrypts the IoV information as ? Re-generates message authentication code as = , and checks . If holds the integrity test holds and then accepts the IoV information mi;t otherwise rejects the factor I, respectively. The incentive and trust factors models are described as follows:

(

(2) where is the incentive given to the source by the destination node, Ii is the previous trust factor of the source node, Tnbh is the total number of previous blackhole attacks launched by are the black-hole, worm-hole, and integrity attacks weights, respectively, are the corresponding black-hole, worm-hole, and integrity attacks launched status.? = (s2+s3)s1 1 + (s1+s3)s2 2 + (s1+s2)s3 3 I i+1 = I i + (1 ? e ?T nbh) + T nbh e ?i ? d ?i = ? r d i e(r d P, r i P) = e(P, P) r d ri m i,t = D ? d ?i (c i,t) ? H ? (m i,t) d ?i ? ? = ?

To detect and dissuade black-hole attacks, we develop an incentive and trust models as shown in equation 1 and 2. These models are used by the destination and edge to compute incentive and trust At the clearance of source node of worm-hole attack, successful black hole and integrity tests, the destination node computes the incentive using Eqn 1, encrypts the computed incentive as , using the next unused master secret key from its master secret key chain, and sends it to the edge. The edge decrypts the , updates the source node trust factor

using equation 2, and pushes a copy of the updated trust factor table and the IoV data to the cloud server for other entities outside the edge coverage.? ? i, 1 , 2 , 3

8 V. Results and Discussions

In this section, we presented the experimental results for the proposed scheme in terms of communication and computation overheads incur as a result of the execution of the scheme.

The experimental set-up evaluates the computation and communication costs. To achieve this, we simulate each of the cryptographic operations used in the proposed scheme using a cryptoPP library [?] implemented on Intel(R) Core(TM)i3 2.73GHz.

The simulation shows that an exponentiation operation in G (Te) takes 5.5ms, a bilinear pairing operation (Tbp) takes 11.07ms, 256-bit Rijndael symmetric encryption (Tse) takes 1.9348ms, 0:007ms as the running time of a general hash function operation (TH), and a scalar multiplication operation (Tsm) takes 2.165ms. With the these cryptography operations running times, the set-up phase takes Tbp + Te + (m0 + 1)TH = 16:807ms for any registered entity, while the edge and cloud each take tbp = 11:07ms. Meanwhile, in the IoV data hopping phase for a hop count, source takes 2Tse+Te+TH = 7:442ms while the destination node requires (h" + 2)TH + Tse + Te + Tdec = 19:184ms. Figure **??** shows the summary of the computation overheads of each phases in terms of running time.

We also evaluate the communication overhead of the scheme. We notice that the source node incurs bits as the communication overhead during IoV data hopping where is the number of periodic-slices used, is the size of a periodic-slice, jHj is the size of the hash function, and jcj is the size of the ciphertext. The attacks detection and integrity test phase incur jHj+jGj bits. That is, the total communication overhead of the scheme is n0jtj + 4jHj + jcj + jGj = 232 bytes for 256 bits ciphertext of Rijndael symmetric encryption, periodic-slice of size 16-bit, of 512-bit size group G, and 256-bit SHA-256. This reflects that the proposed scheme only has an insignificant communication overhead.

The proposed incentive and trust factors model are evaluated in terms of how different attack patterns A= "black hole, worm-hole, integrity" affects the incentive and trust of source node with initial trust value I=50, where "0" represents attack and "1" represent no attack. Figure **??** shows the incentives of source nodes launching different patterns of black-hole, wormhole, and integrity attacks. It indicates that any instance of attack reduces the incentive and both worm-hole and blackhole attacks significantly reduce the source node incentive at an instance of integrity attack. Figure **??** depicts the effect of different attacks of different patterns on the trust values of the source node. It implies that the scheme assigns the highest trust value for a source node with no record of attack in the network. That is, it indicates a good reputation for the source node with no or few records of attacks. Also, the mean waiting time of the destination node for different network sizes and one-time key chains are shown in Figure **??**. It shows that the network size does not affect the mean waiting time, that is with the increase in the network size the proposed scheme introduces insignificant delay. However, there is a significant delay as the entity's time key chain increases.

9 Global Journal of Computer Science and Technology

Volume XXII Issue I Version I [1]

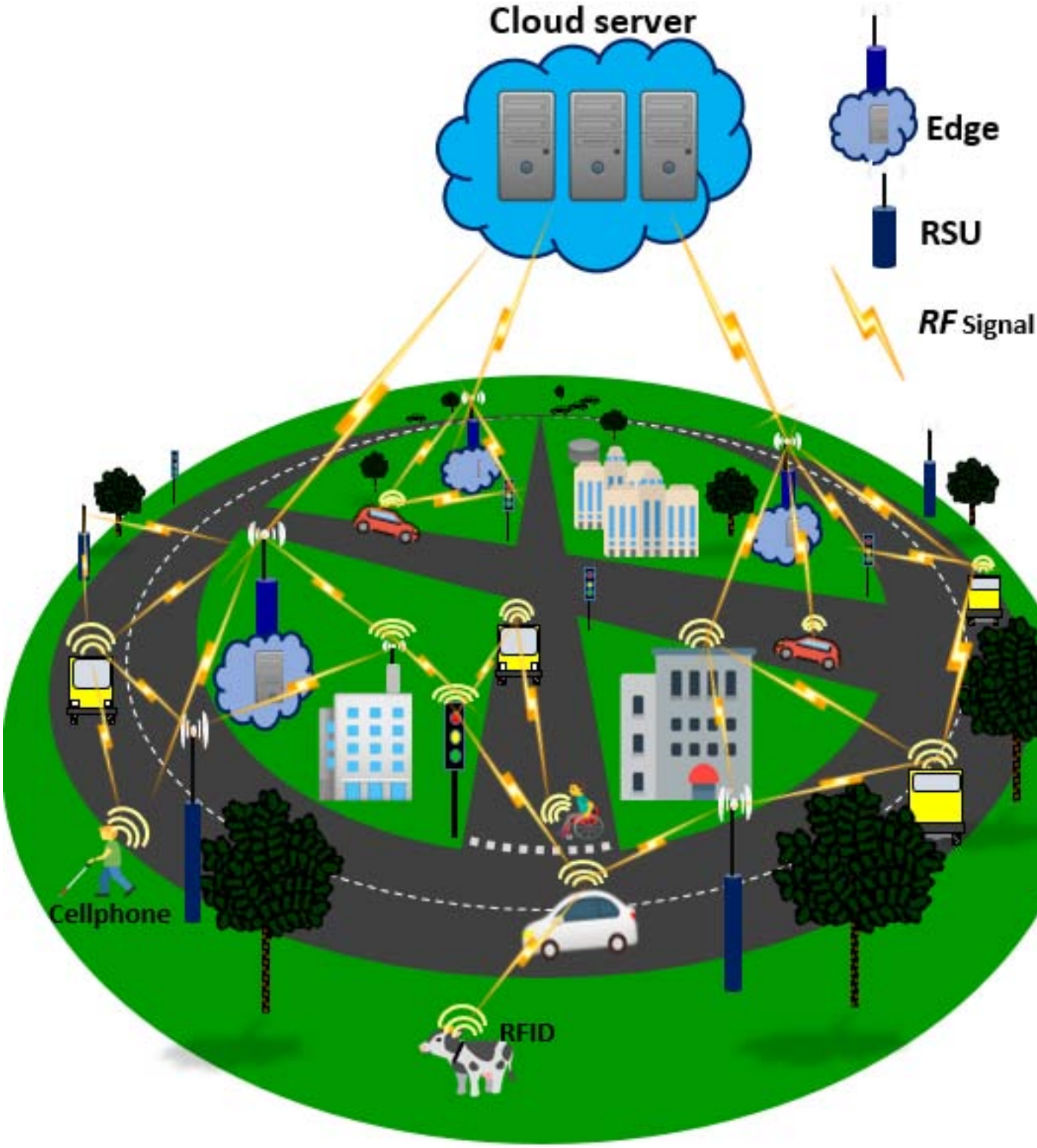
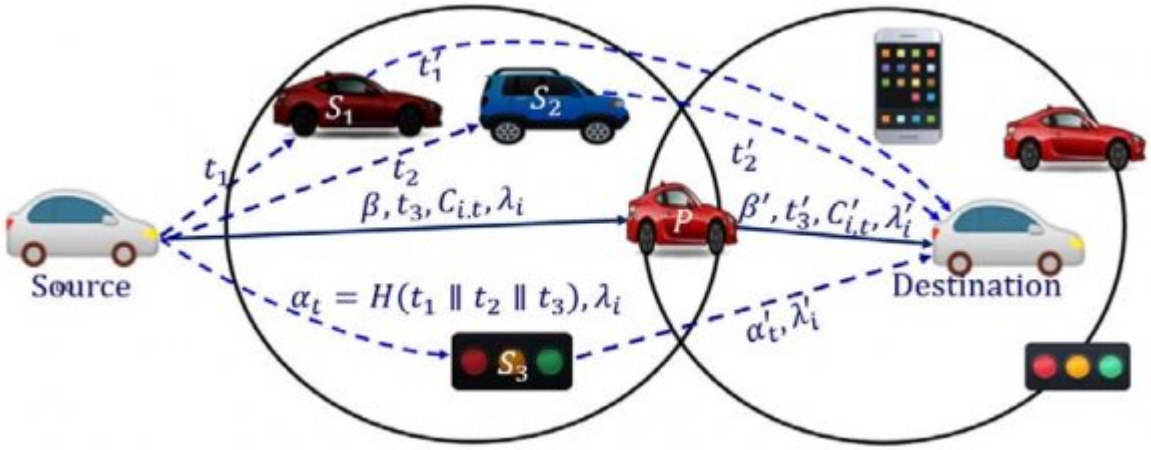
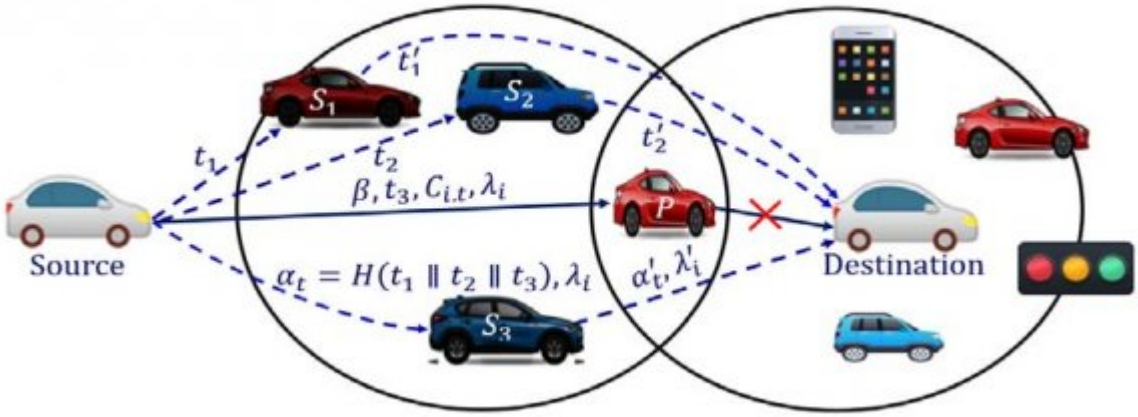


Figure 1:



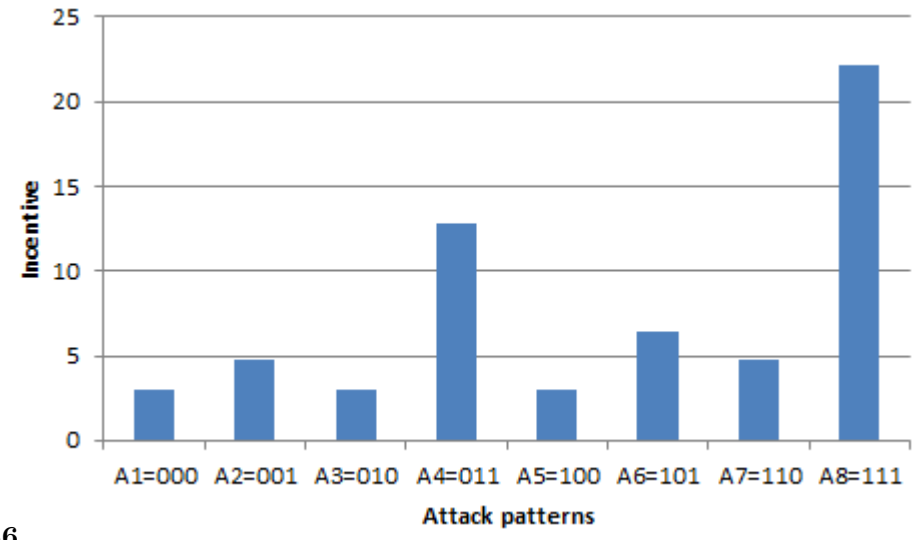
1312

Figure 2: s 1 , s 2 , s 3 d)Fig. 1 :Fig. 2 :



34

Figure 3: Fig. 3 :Fig. 4 :



56

Figure 4: Fig. 5 :Fig. 6 :

I

Year 2022
32
Volume XXII
Issue I Version
I
( ) B

Notation	Description
Zq	set of integer of order p
G	addition group of order q
P	generator of G
H k (.)	key based hash function
I	trsut factor
?	incentive value
? i	pseudonym of entity i
n'	number of selected secondary nodes
? i	encrypted pseudonym of i
?	message authentication code
e	bilinear mapping function

[Note: j , ? i , ? d , ?c mutual public key parameter of i, j, d, and c, respectively ? imaptoj , ? cmaptoj entity-edge mutual secret key, cloud-edge mutual key ? one-time-key chain]

Figure 5: Table I

This paper proposed a new method to detect the black hole, worm-hole, and integrity attacks during communication in an IoV environment and assigns high trust and incentive to an honest entity but low or no trust and incentive to a malicious entity.

.1 References Références Referencias

[Sun et al.] , Y Sun , L Wu , S Wu , S Li , T Zhang , L Zhang .

[Biswas and Misic (2013)] 'A Cross-Layer Approach to Privacy-Preserving Authentication in WAVE Enabled VANETs'. S Biswas , J Misic . *IEEE Transactions on Vehicular Technology* Jun. 2013. 62 (5) p. .

[Wahab et al. (2014)] 'A Dempster-Shafer based tit-fortat strategy to regulate the cooperation in VANET using QoS-OLSR protocol'. O A Wahab , H Otrok , A Mourad . *Wireless Pers. Commun* Apr. 2014. 75 (3) p. .

[Safi et al. ()] 'A novel approach for avoiding wormhole attacks in VANET'. S M Safi , A Movaghar , M Mohammadizadeh . *2009 First Asian Himalayas International Conference on Internet*, 2009. p. .

[Sakiz and Sen ()] 'A Survey of Attacks and Detection Mechanisms on Intelligent Transportation Systems: VANETs and IoV'. Fatih Sakiz , Sevil Sen . *Ad hoc Network* 2017. 61 p. .

[Cui ()] 'Attacks and countermeasures in the internet of vehicles'. X Cui . doi:10.10 07/s12243-016-0551-6. *Annals of Telecommunications* 2016. 72 (5-6) p. .

[Cherkaoui et al. ()] 'Black-hole Attack Detection in Vehicular Ad Hoc Networks Using Statistical Process Control'. Badreddine Cherkaoui , Abderrahim Beni-Hssane , Mohammed Erritali . *International Journal on Communication Antenna and Propagation* 2017. 7 (3) .

[Baiad et al. (2014)] 'Cooperative crosslayer detection for blackhole attack in VANET-OLSR'. R Baiad , H Otrok , S Muhaidat , J Bentahar . *Proc. Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)*, (Int. Wireless Commun. Mobile Comput. Conf. (IWCMC)Nicosia, Cyprus) Aug. 2014. p. .

[Sanadiki et al. ()] 'Detecting attacks in QoS-OLSR protocol'. H Sanadiki , H Otrok , A Mourad , J.-M Robert . *2013 9th International Wireless Communications and Mobile Computing Conference (IWCMC)*, 2013. p. .

[Khan et al. (2015)] 'Detection of malicious nodes (DMN) in vehicular ad-hoc networks'. U Khan , S Agrawal , S Silakari . *Procedia Comput. Sci* Jan. 2015. 46 p. .

[Daeinabi and Rahbar (2013)] 'Detection of malicious vehicles (DMV) through monitoring in vehicular ad-hoc networks'. A Daeinabi , A G Rahbar . *Multimedia Tools Appl* Sep. 2013. 66 (2) p. .

[Delkesh and Jamali ()] 'EAODV: Detection and removal of multiple black hole attacks through sending forged packets in MANETs'. T Delkesh , M Jamali . *J. Ambient Intell. Hum. Comput* 2019. 10 (5) p. .

[Hortelano et al. (2010)] 'Evaluating the usefulness of watchdogs for intrusion detection in VANETs'. J Hortelano , J C Ruiz , P Manzoni . *Proc. IEEE Int. Conf. Commun. Workshops*, (IEEE Int. Conf. Commun. WorkshopsCapetown, South Africa) May 2010. p. .

[Hu et al. ()] 'Packet leashes: a defense against wormhole attacks in wireless networks'. Y C Hu , A Perrig , D B Johnson . *INFOCOM 2003. Twenty-Second Annual Joint Conference of the IEEE Computer and Communications*, 2003. IEEE Societies. 3 p. .

[Hu et al. (2003)] 'Packet leashes: a defense against wormhole attacks in wireless networks'. Y Hu , A Perrig , D B Johnson . *Proceedings of the 22 nd Annual Joint Conference on the IEEE Computer and Communications Societies*, (the 22 nd Annual Joint Conference on the IEEE Computer and Communications Societies) April 2003. 3 p. .

[Kadam and Limkar ()] 'Performance investigation of DMV (detecting malicious vehicle) and DPMV (detection and prevention of misbehave/malicious vehicles): Future road map'. M Kadam , S Limkar . *Proc. Int. Conf. Frontiers Intell. Comput., Theory Appl. (FICTA)*, (Int. Conf. Frontiers Intell. Comput., Theory Appl. (FICTA)) 2014. p. .

[C ? Apkun et al. ()] 'SECTOR: secure tracking of node encounters in multi-hop wireless networks'. S C ? Apkun , L Buttya´n , J. -P Hubaux . *Proceedings of the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)*, (the 1st ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '03)Fairfax, Va, USA) 2003. p. . (View at: Publisher Site -Google Scholar)

[Eriksson et al. (2006)] 'TrueLink: a practical countermeasure to the wormhole attack in wireless networks'. J Eriksson , S V Krishnamurthy , M Faloutsos . *Proceedings of the 14th IEEE International Conference on Network Protocols (ICNP '06)*, (the 14th IEEE International Conference on Network Protocols (ICNP '06)) November 2006. p. .

[Yao et al. (2017)] 'Using trust model to ensure reliable data acquisition in VANETs'. X Yao , X Zhang , H Ning , P Li . *Ad Hoc Networks* Feb. 2017. 55 p. .

[Yao et al. (2017)] 'Using trust model to ensure reliable data acquisition in VANETs'. X Yao , X Zhang , H Ning , P Li . *Ad Hoc Netw* Feb. 2017. 55 p. .