Special Issue on Chemistry

Computationally Productive Security Saving Verification and Key Circulation Methods for Vehicular Specially Appointed Systems

R. Kalpana and G. Padmapriya

Issue Editor
Dr. A. Manikandan

Research Journal of Agricultural Sciences
An International Journal

P- ISSN: 0976-1675
E- ISSN: 2249-4538

Volume: 13
Issue: Special

Res. Jr. of Agril. Sci. (2022) 13(S): 047–049

CARAS

Res. Jr. of Agril. Sci. (2022)
13(Special): 047–049

ISSN: 0976-1675 (P)
ISSN: 2249-4538 (E)

www.rjas.org

Full Length Research Article

Computationally Productive Security Saving Verification and Key Circulation Methods for Vehicular Specially Appointed Systems

R. Kalpana[1] and G. Padmapriya*[2]

Received: 16 Nov 2021 | Revised accepted: 05 Feb 2022 | Published online: 25 Feb 2022

ABSTRACT

The incorporation of electronics by embedding the relevant sensors in the physical devices in home and office, vehicles of all types, buildings in the smart cities and in all possible spheres of life form a network of devices termed as internet of things (IoT). It is being realized that vehicular ad-hoc networks (VANETs) which are responsible for the reliable and secure communication among vehicles is a primary area of research in IoT and hence ensuring security in this area is essential. Thus, this work introduces a novel approach to improve the existing authentication support to VANETs. In this proposed framework, first an anonymous authentication approach for preserving the privacy is proposed which not only performs the vehicle user's anonymous authentication but preserves the message integrity of the transmitting messages as well. Although many anonymous authentication schemes have been proposed in VANETs until now, the existing schemes suffer from a high computation cost during the signature and certificate verification process which leads to delayed authentication. Consequently, the vehicles and roadside units (RSUs) cannot authenticate more number of vehicles per second in VANETs. Second, an efficient anonymous group key distribution protocol is proposed in this paper for securely distributing the group key to the group of vehicles in the communication range of an RSU. The RSUs can send location-based information to the group of vehicles in a secure manner using this group key. Experimental analysis portrays that the results of this new privacy preserving anonymous authentication and key management schemes are promising and efficient with regard to signature verification cost and computational cost in comparison with the existing schemes.

Key words: Sensors, Physical devices, VANETs

A story light weight Protocol by name Anonymous Authenticated Secure - Selective Design Relay Inquiry Protocol (AAS-SELDRIP) that can diminish the overhead in the data dispersal process and to make the dissipating system secure in an appropriated space has been proposed at the present time [1-4]. The amount of social events made is direct relating to the thickness of the passed on sensor center points. AAS-SELDRIP has been organized so it perceives the sensor center points in each get-together which are requiring data dispersing and allows the framework customer of each social event to spread the data things using multi bob correspondence without uncovering its character [5]. The system client ought to get selected with the BS and get Dissemination Privilege (DP) to go about as a system client. The supposition that will be that the system client performs dispersal through generally top of the line gadgets like cell phones, note pad PCs, PCs and so forth. The principal obligation of the system client is to include the part hubs, produce keying materials and perform information dispersal [6]. The DP of each system client in the comparing bunch are preloaded with its gathering sensor hubs. The system client has power over the current part hubs to evacuate whenever saw as noxious and to include new part hubs if the circumstance requests. The connection between the system client and passage is comparable to the connection between the system client and the BS as far as appointing the system keys. Before information scattering the system clients of each gathering ought to enlist with door to get the transitory character factors.

The gateway consists of Large Key Space (LKS) which has the ability to generate keys and store temporary identity variables for the network users [7]. Another assumption is that gateways are protected by using tamper resistant hardware, where offline and key guessing attacks are not possible [8]. The information spread in the appropriated condition is performed by the system clients with the assistance of base station and the procedure is intended for the sensor hubs. The BS disperses the obligations of playing out the information spread to arrange client by assigning a gathering of sensor hubs to every client dependent on land area [9].

MATERIALS AND METHODS

* G. Padmapriya
✉ ppstminex@gmail.com

[1-2] Department of Chemistry, Bharath Institute of Higher Education and Research (BIHER), Chennai - 600 073, Tamil Nadu, India

Packet transmission and verification phase

The corresponding network user of each group constructs an appropriate Data Dissemination Packet (DDP) to all member nodes which are in need of data dissemination. The packet format of DDP is given in Equation (4).

$$DDP = (T, DP, VN, D) \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (4)$$

Where, DDP is Data Dissemination Packets, T is Time stamp, DP is Dissemination Privilege of the corresponding network user of a group, VNis Version number of data items and Dis Data items.

Once the DDP is constructed the network user of each group uses AES algorithm to encrypt the data dissemination packets with its generated secret key and sends it to the interested member nodes. Many DDPs are combined together to form the Data Dissemination Message (DDM) and format of an encrypted DDM is shown in Equation (5).

$$DDM_E = h\ (DDP \parallel NU_{SK}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots.. (5)$$

Where, DDM_E is Encrypted Data Dissemination Message, h (.) is Collision resistant hash function, DDP is Data Dissemination Packets and NU_{SK} is secret key of the corresponding network user of each group. In packet verification phase, we consider the gathering part hubs as the recipients which have mentioned the information spread from their system client. After getting the information dispersal message from the legitimate relating system client of each gathering, a relating bunch part hub checks whether the timestamp Ti remembered for Data Dissemination Packet (DDP) is inside passable range contrasted and current time [10 - 13]. In the event that it can't, Data Dissemination Message (DDM) is dismissed.

Table 1 Simulation parameters

Network simulator	NS2 version (2.29) Mannasim framework
Simulation area	1000m*1000m
Density of nodes	125-500
Transmission range	15-20m
Physical layer	Phy/wirelessphy-mica2
Radio propagation model	Two ray model
Environment	Urban
Nodeinitial energy	100J
Transmission power(tx)	1 J per packet with maximum power
Receiving power (rx)	0.25J per packet with maximum power
Simulation duration	60 minutes
No of trails	60
Packet size	50-300 bytes

RESULTS AND DISCUSION

From our recreation we saw that normal vitality devoured by the system for differing bundle sizes fluctuates from 0.14J to 0.23J every moment and henceforth the vitality utilization changes between 9J to 13.8J every hour. Also, we saw that within the sight of malignant hubs the vitality utilization has changed from 12J to 20J every hour. ADE is estimated with changing parcel sizes. From the diagram, we see that Average Dissipated Energy (ADE) of AAS-SELDRIP is less when contrasted and other information dispersal conventions. AAS-SELDRIP convention chooses the hubs which are needing information dispersal and finds ideal steering way by to spread the information things.

DI - DRIP and SE-DRIP utilize the stream calculation which floods the information things to the sensor hubs to perform information spread. In this manner Average Dissipated Energy (ADE) of these conventions is more when contrasted and AAS-SELDRIP. The Average Dissipated Energy of AAS-SELDRIP, DI-DRIP and SE-DRIP with ordinary hubs and vindictive hubs. Within the sight of noxious hubs the proposed plans has devoured less ADE. From the diagram, we see that Average Dissipated Energy (ADE) of AAS-SELDRIP is better contrasted and S-SELDRIP in light of the fact that AAS-SELDRIP furnishes security by symmetric key cryptosystem with AES calculation. Though in S-SELDRIP it furnishes security by open key cryptosystem with advanced mark. Thefore, in AAS-SELDRIP has better computational and communication overhead compared with S-SELDRIP. Hence it has better ADE compared with S-SELDRIP.

We observe that AAS-SELDRIP has better dissemination ratio compared with S-SELDRIP because AAS-SELDRIP has better computation and communication overhead during transmission of control packets, data packets and key exchanges. Hence the dissemination ratio of AAS-SELDIP exhibits better performance in terms of dissemination ratio

CONCLUSION

In this paper the AAS-SELDRIP convention which gives the specific and secure information dispersal by distinguishing the intrigued sensor hubs preceding the information scattering action in the disseminated condition by utilizing the standards-based directing has been proposed, broke down and assessed. The proposed convention gives the safe directing and takes out the Redundant Broadcast Storm Problem (RBSP) and improves the exhibition of the system by distinguishing the malevolent hubs and recoveries the vitality of the system during the information spread. Results shows that proposed AAS-SELDRIP performs better with other existing protocols with performance metrics like ADE, DR, TFND, End to End Delay, routing overhead and throughput and has better Attack Detection Accuracy compared with existing data dissemination protocols.

LITERATURE CITED

1. Dong, W, Chen, C, LiuxTeng, G, Buj& Livy 2012, ‘Bulk Data Dissemination in Wireless Sensor Networks: Modeling and analysis’, Computer Networks, vol.56, no.11, pp. 2664-2676.
2. Dongo, W, Chen, C, LiuxBuj&Gao, Y 2011, ‘A Light Weight and Density aware Reprogramming Protocols for Wireless Sensor Networks’, IEEE Transactions on Mobile Computing, vol.10, no.10,pp.1403-1415.
3. Du, W, Deng,J, Han,YS &Varshney,PK 2003, ‘A pair wise key pre distribution scheme for wireless sensor networks’ , In Proceedings of the 10th ACM Conference on Computer and Communications , pp. 42-51.
4. Du, X, Xiao,Y,Guizani,M, Chen,HH 2007, ‘An Effective Key Management Scheme for Heterogeneous Sensor Networks’ , Ad Hoc Networks, vol. 5, no. 1, pp. 24-34
5. Ehsan Ahvar, René Serral-GraciàEva, Marín-Tordera, Xavier Masip- Bruin & Marcelo Yannuzzi 2012, ‘EQR: A New Energy-Aware Query-Based Routing Protocol for Wireless Sensor Networks’, International Conference on Wired/Wireless Internet Communications, pp.102-110.
6. Eschenauer, L &Gligor,VD ‘A key management scheme for distributed sensor networks’, In Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 41-47.
7. Dong, W, Chen, C, LiuxTeng, G, Buj& Livy 2012, ‘Bulk Data Dissemination in Wireless Sensor Networks: Modeling and analysis’, Computer Networks, vol.56, no.11, pp. 2664-2676.
8. Dongo, W, Chen, C, LiuxBuj&Gao, Y 2011, ‘A Light Weight and Density aware Reprogramming Protocols for Wireless Sensor Networks’, IEEE Transactions on Mobile Computing, vol.10, no.10,pp.1403-1415.
9. Du, W, Deng,J, Han,YS &Varshney,PK 2003, ‘A pair wise key pre distribution scheme for wireless sensor networks’ , In Proceedings of the 10th ACM Conference on Computer and Communications , pp. 42-51.
10. Du, X, Xiao,Y,Guizani,M, Chen,HH 2007, ‘An Effective Key Management Scheme for Heterogeneous Sensor Networks’ , Ad Hoc Networks, vol. 5, no. 1, pp. 24-34
11. Ehsan Ahvar, René Serral-GraciàEva, Marín-Tordera, Xavier Masip- Bruin & Marcelo Yannuzzi 2012, ‘EQR: A New Energy-Aware Query-Based Routing Protocol for Wireless Sensor Networks’, International Conference on Wired/Wireless Internet Communications, pp.102-110.
12. Eschenauer, L and Gligor, VD ‘A key management scheme for distributed sensor networks’, In Proceedings of the 9th ACM Conference on Computer and Communication Security, pp. 41-47.