Scalable Computing: Practice and Experience, ISSN 1895-1767, http://www.scpe.org
© 2020 SCPE. Volume 21, Issue 1, pp. 101–105, DOI 10.12694:/scpe.v21i1.1626

SPCACF: SECURED PRIVACY-CONSERVING AUTHENTICATION SCHEME USING CUCKOO FILTER IN VANET

A. RENGARAJAN *AND MOHAMMED THAHA M. †

Abstract. Providing security for vehicular communication is essential since the network is vulnerable to severe attacks. The message authentication between vehicles and pavement units are essential for the purpose of security. Messages that passed between the vehicles should be encrypted and verified before the vehicle nodes could be trusted. The original identity of nodes can only be traceable by authorized parties and should not be exposed at any cause. However authentication between vehicles during message transformation does not guarantees message authentication rate accurately. To address these issues, the SPCACF scheme is proposed which is based on software devoid of relying on any particular hardware. Binary search algorithm is added in partial with Cuckoo Filter to achieve higher accomplishment than the preceding schemes in the batch wise verification phase. In order to guarantee that it can assure message authentication constraint, existential enforceability of underlying signature against adaptively chosen-message attack is proved under the positive filter pool method.

Key words: Message Filters, Vehicular Ad hoc Networks, Authentication, wireless.

AMS subject classifications. 68M15

1. Introduction. The systems that interconnect vehicles on road are called Vehicular Adhoc NETwork (VANET). "A portable impromptu system comprises of versatile nodes that associate themselves in a decentralized, self-sorting out and may likewise set up multi-hop paths. In the event that versatile nodes (cars) are movable, this is called VANET". "The fundamental focus of research in VANETs is the upgrades of vehicle security by methods for Inter Vehicular Correspondence (IVC)".Several different applications are emerging in VANETs [1-3]. These 3 applications incorporate security applications to make driving a lot more secure, portable trade and other data benefits that will illuminate drivers about any sort regarding blockage, driving risks, mishaps, roads turned parking lots. VANET technology uses moving vehicles as nodes in a network to create a mobile network. VANET turns each taking an interest vehicle into a remote switch or hub, permitting cars around 100 to 300 mts from one another to connect and make a system with a wide range. As vehicles drop out of the sign range and drop out of the system, different vehicles can participate, connecting vehicles to each other with the goal that a versatile system is made [4]. It is assessed that the main frameworks that will incorporate this innovation are police and fire vehicles to communicate with one another for security related purposes.

2. Related Works. VANETs had updated in several ways for faster communication among vehicles. The main difference between MANET and VANET is that the MANET has mobile routers that act as nodes for transmission of message and those routers builds VANET system using vehicles.

In network communication, a topology is a typically schematic depiction of the arrangement of a system, including its nodes and interfacing lines. There are two different ways of characterizing system geometry: the physical topology and the logical (or sign) topology. The physical topology of a system is the real geometric design of workstations. Logical (or signal) topology alludes to the idea of the ways the sign pursue from node to node. The vehicle shares their sensed message and location information for changing the traffic flow and controlling it in a futuristic manner.

*Professor, Vel Tech Multitech Dr Rangarajan Dr Sankutala Engineering College, Avadi, Chennai 600062, India. (rengu_rajan@yahoo.com)

†Assistant Professor, B.S.Abdur Rahman Cresent Institute of Science and Technology, Chennai, India (thkadiri@gmail.com)

For reliable communications localization is a major challenge in achieving reliable communication in WSN. Sensor node position is termed as localization and non-linear version of Extended Kalman filtering deals with the case governed by stochastic degree of difference equations, This filter have consistency issues. Efficient algorithm for sensor locality enables to estimate the location with high accuracy. Particle swarm optimization assisted EKF for localization in WSN. A few distinct applications are rising as to vehicular communications that are mainly based on the fingerprint recognition for secured data communication [5-7]. For instance, applications for more secure driving, data administrations to educate driver's business benefits in the vehicle region. Government, organizations, and the scholastic networks are taking a shot at empowering new applications for VANETs. A primary objective of VANETs is to build street security by the utilization of remote correspondences. To accomplish these objectives, vehicles go about as sensors and advise each other about irregular and conceivably destructive conditions like mishap, car influxes and coats. Vehicular systems intently look like specially appointed systems on account of their quickly changing topology [8, 9] by applying filter techniques. For various regions there exist trust agents in order to provide secured keys for secured communication. There are numerous elements engaged with a VANET settlement and sending. Despite the fact that by far most of VANET fundamental tasks in those systems performed with various substances [10]. Selection mechanism was proposed to identify the Line of Sight and Non-Line of Sight conditions. Here hybrid EKF and H-infinity filter is used to look up the accuracy. Finally we use linear least square algorithm to estimate the location [11]. Iterative filtering algorithm (IF) was proposed and the data is grouped concurrently from various sources and IF moreover cause to be trust evaluation of sources. Using weight factors assigned to data trust evaluations are done. Security is considered as a major issue therefore an improved IF method was proposed by providing approximation. IF algorithm [12] will improve the system performance potentially in WSN, IF includes security factor algorithm with novel method for collusion detection and revocation on the basis of primary aggregation of statistics values with various distribution.

3. SPCACF - Description.

3.1. Node Creation and Configuration. Node creation is only the production of the nodes wirelessly in the system that is chosen. Node configuration system basically comprises of characterizing the diverse hub attributes before making them. They may comprise of the kind of tending to structure utilized in the recreation for characterizing the system segments of portable nodes.

3.2. Neighbor node Discovery. Each wireless node finds its neighboring nodes, the ones that are within its transmitting range. Neighbor discovery in a WSN is the determination of all nodes with which a given node may communicate directly. On the contrary, neighbor discovery reveals all possible paths between any two nodes in a network. Neighbor discovery is achieved by the conditions specified in this paper: using distance and the number of hops conditions.

3.3. Initial handshaking and Message signing. When vehicle enters into new Road Side Unit (RSU) then initial progress of handshaking should be carried out. Through the use of RSU the vehicles substantiate itself with trust authority. Trust authority is the main tool to recognize the nodes original distinctiveness or ID. Trust authority will pass message to roadside unit to allow it to verify the vehicle's signature even if it uses pseudo identity for message signing. Trust authority has two filters such as positive filter pool and negative filter pool and it generates secret key with the vehicle. RSU will forward shared secret from the positive filter pool to the automobile. Each vehicle generates secret integer when moving to each new RSU.

3.4. Group key signing and verification. RSU utilizes this module to check a lot of messages without the bilinear matching tasks in a group mode. Creating a notification communicate message utilizing cuckoo filter is presented along with working instance of invalid signatures in the batch verification is clarified in this scheme.

4. SPCACF Algorithm - Description. Secured privacy-conserving authentication model for VANETs along with Cuckoo Filter is used to improve the network security features. Cuckoo Filter along with binary search methods which accomplish advanced progress rate than the earlier schemes in the batch verification stage. Binary search consists of positive filter pool and negative filter pool for verification purpose. The vehicles should get paired before them starting communication.

Let V_i be the source vehicle and V_j be the sink vehicle. V_i computes fingerprint signature and sends to the node V_j, now V_j computes fingerprint signature and sends back to the node V_i. V_i checks for the positive and negative filters on the binary search basis. If the fingerprint signature of both nodes F_i and F_j falls under positive filters and also get matched, then the set of data transmission is done and the query is passed to some other vehicles present in the road side units.

The generated signature by the source node falls under the positive filter pool and it contains some integers with it. Also the negative filter pool consists of some integer representation indicates malicious fingerprint signature. If the sink's signature falls under the positive filter pool, then the source can send the requested information (M_i, σ_i) to the destination. But the signature falls under the negative filter pool then the source vehicle V_i needs to re-confirm with the V_j. The data cannot be processed since the node V_j marked as malicious vehicle.

$$X_{j,i} = (ID_j \parallel T_j \parallel M_j) \tag{4.1}$$

Algorithm SPCACF
Require: $X_{j,i}$ <- ($ID_j \parallel T_j \parallel M_j$).
1: Vi computes a fingerprint fj <- Fingerprint(xj)
2: Vi queries Cuckoo Filters with query.
3: Vi checks novelty of Ti.
4: While $T_i - T_j \leq \Delta T$ Do
5: Vi checks fj against Cuckoo Filters;
6: if fj is in positive Filters then
7: Vi checks fj against negative Filters
8: if fj is not in negative Filters then
9: Vi send (Mi, σ_i) to Vj ; split;
10: end if
11: else
12: if fj presents in negative Filters then
13: Vi re-verification required; split;
14: else
16: if fj present in negative Filters then
17: Vi discards Vj ; break;
18: end if
19: end if
20: else
21: Vi wait for subsequent relay; split;
22: end if
23: end while
24:end

5. Results and Discussions. System performance is evaluated by tracing the files of an output through generated Xgraph files of version NS-2.35. The events occurred in the network animator window are testimony into trace files while accomplishing record process. The events like packet delivery rate, lost rate and residual energy of the different schemes considered in the proposed work and conventional scheme can be traced out using the trace files.

Delivery Rate: DR is defined as the proportion of total data packets established by the sink to total sent packets by source in multiplication with the number of receivers. Delivery rate is calculated by the equation 5.1:

$$PDR = \frac{Total\ Pack\ Received}{Total\ Pack\ Send} \tag{5.1}$$

Loss Rate The Loss Rate is the proportion of packets that failed while reaching the receiver to the sum of data packets sent by the sender. The LR is calculated by Equation 5.2:

$$PLR = \frac{Total\ pack\ Dropped}{Total\ pack\ Sent} \tag{5.2}$$

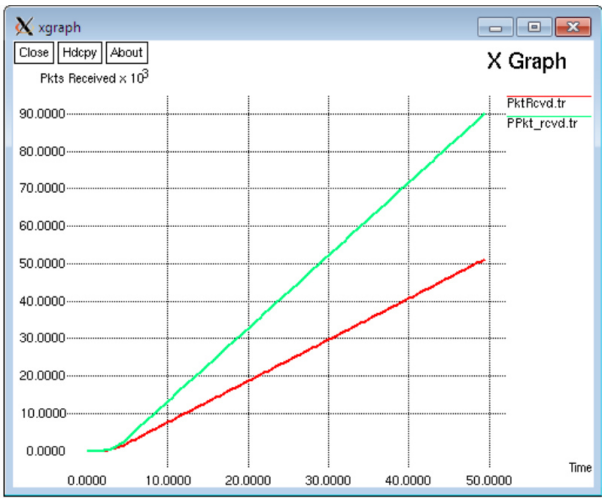

FIG. 5.1. *Delivery rate Vs Time*

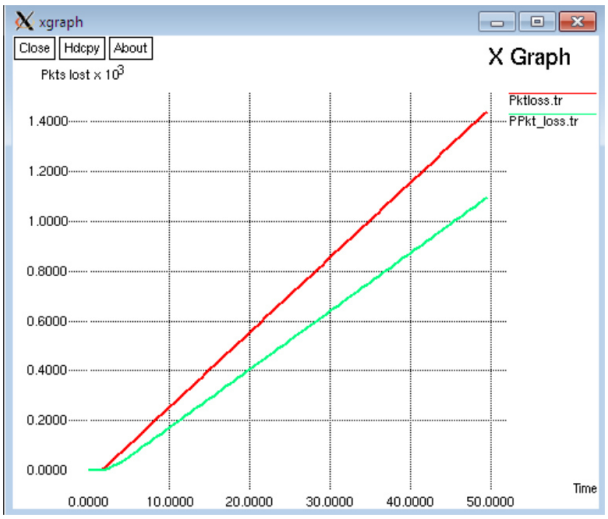

FIG. 5.2. *Loss rate*

Energy Consideration: WSN comprises of sensor nodes fixed over a geological region for observing physical conditions like temperature, mugginess, vibrations, seismic occasions, etc. Normally, a sensor node is a little device that incorporates three essential parts: a detecting subsystem for information obtaining from the physical encompassing condition, a processing subsystem for nearby information preparing and capacity, and a wireless correspondence subsystem for information transmission. What's more, a power source supplies the vitality required by the device to play out the modified undertaking.

Residual energy can be computed from the initial energy of the node. The difference between the initial energy level and the current energy level gives the remaining energy of the node. Figure 5.3 shows residual energy for both proposed and existing method.

6. Conclusion. Secured privacy-conserving authentication scheme with cuckoo filter utilized for both between vehicles communications and vehicle to roadside communications. Positive and negative filter pool is established for verifying the integer keys by applying binary searching process. This improves the efficiency of the proposed scheme through batch validation process. The performance analysis results show that the proposed scheme has better efficiency when compared with existing schemes. Internet of Things can be included for the

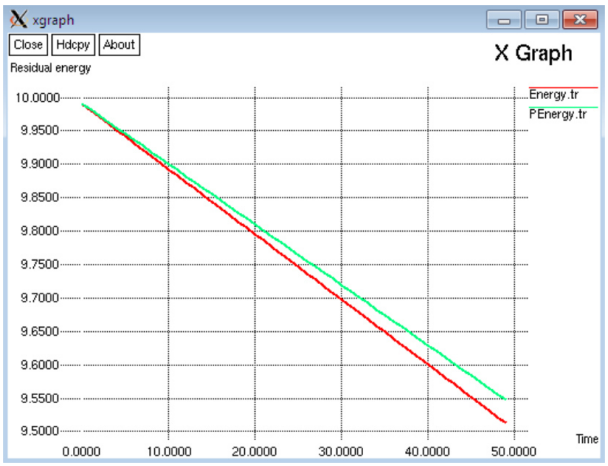

FIG. 5.3. *Residual energy*

further development of application in the case of achieving secured circumstances.

REFERENCES

[1] L. L.AYUAN AND L.CHUNLIN, A Qos multicast routing protocol for clustering mobile ad hoc networks. Computer Communications, 307(2007), pp, 1641-1654.
[2] X. YANG,J. LIU, F.ZHAO, AND N. VAIDYA, "A vehicle- to-vehicle communication protocol for cooperative collision warning," Proc.Int.Conf.MobiQuitous,2004,114-123.
[3] K. D. WONG, K.TEPE, W. CHEN, M.GERLA, "Inter Vehicular communication," IEEE wireless Communications,vol.13,issue no.5,October 2006.
[4] NANDAN, S.DASS,G.PAU, M.Y.SANADIDI, M. GERLA, "Car Torrent: A Swarming Protocol for vehicular networks", IEEE INFOCOM, Miami, Florida, March 2005
[5] J. NZOUONTA, C. BORCEA, "STEID: a Protocol for Emergency Information Dissemination in Vehicular Networks", Report, Department of Computer Science, New Jersey Institute of Technology, 2006
[6] J.ZHAO AND G. CAO, "VADD: Vehicle-assisted data delivery in vehicular ad hoc networks," IEEE Transaction Vehicular Technology, Vol.57, N0.3,pp. 1910-1922, May 2008
[7] R.AHLSWEDE, N. CAI, S.Y.R. LI, AND R.W. YEUNG, "Network Information flow, " IEEE Transactions on Information Theory, vol.46, no. 4, pp.1204-1216,2000
[8] M. SARDARI, F. HENDESSI, AND F.FEKRI, "DDRC: Data Dissemination in Vehicular Networks Using Rate less Codes", presented at J.Inf.Sci.Eng.,2010,pp.867-881
[9] P. CATALDI, A. TOMATIS, G. GRILLI, AND M. GERLA, "CORP: Cooperative rate less code protocol for vehicular content dissemination", pages 1-7,29 2009-july1 2009
[10] XIUMIN WANG, JIANPING WANG AND V. LEE, " Data Dissemination in Wireless Sensor Networks with Network Coding," EURASIP Journal on Wireless Communications and networking, vol. 2010, Article ID 465915, 14 pagess, 2010.doi: 10.1155/2010/465915.
[11] HU, NAN, CHENGDONG WU, TONG JIA, AND PENG JI. "Hybrid filter localization algorithm based on the selection mechanism." In The 27th Chinese Control and Decision Conference (2015 CCDC), pp. 1128-1131. IEEE, 2015.
[12] CHOUDHARI, EKTA, KETAN D. BODHE, AND SNEHAL M. MUNDADA. "Secure data aggregation in WSN using iterative filtering algorithm." In 2017 International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), pp. 1-5. IEEE, 2017.

Edited by: Swaminathan JN
Received: Oct 29, 2019
Accepted: Jan 28, 2020