Identifying and Securing Malicious Behavior in MANET

Prakash Deshmukh
M.Tech Research Scholar
Computer Science
SIST (Shree), Bhopal

Yogesh Rai
Assistant Professor
Computer Science
SIST (Shree), Bhopal

Santosh Kushwaha
HOD and Assistant Professor
Computer Science
SIST (Shree), Bhopal

ABSTRACT
A mobile ad hoc network (MANET) is auto configurable system. This environment allows us to move haphazardly in any path. These sorts of system are in some cases self-controlled or controlled by any web zone. The usability and opportunity to migrate make this stage a more extensive use in the present system populace. The information accepting and partaking in this environment is making this environment all the more agreeable to utilize and adjust. Be that as it may, adjusting the security system is of more noteworthy concern. So in this paper a hybrid encryption method based on Ron Rivest, Adi Shamir, and Leonard Adleman(RSA) and Rivest Cipher (RC) is applied on the data for protecting it. A has code is also added to recongiges the malicious behavior detection by reckoning it timely. The results also prove the effectiveness of this approach.

Keywords
MANET, Security, RSA, RC, Data sharing and gathering.

1. INTRODUCTION
In light of the development mobile ad hoc network (MANET) is a slanting stage of the communication research. It provides a direction to uproot the constraints of correspondence reach [1]. This framework model presupposes that center points are prepared to pass on development other than their own [2]. Exactly when unrehearsed frameworks are sent in threatening circumstances (vital frameworks), or embody center points that fit in with diverse self-governing substances, a tradition unsecure behavior can't be acknowledged. Unattended contraptions can get the chance to be bartered and drop travel action, remembering the deciding objective to corrupt the framework execution [3]. Also, new customers may misconfigure their devices to reject sending movement, remembering the final objective to spare. This sort of behavior is typically termed hub unfortunate behavior [4]. Multipath controlling allows the establishment of various routes between a lone source and single end center point and when a way breaks a trade way is used instead of dispatching another course revelation, along these lines multipath guiding identifies with an ensuring directing strategy for remote adaptable offhand systems [6]. So the first point is to exploit multipath path to the spoke to hubs. At that point the security concern must be considered [7].

This paper focuses on and discusses the game plan for dependable information, transportation considering the versatility of the dynamic nodes a certifiable concern. The nodes with most significant piece to go on the information, isolate the sending zone, with a longing of minimizing the deferral. Later in the run of the safe node of the end vehicle the information gatherings are telecasted until they fulfill the end vehicle. Sending zone and expected zones are circles, the compass for sending circle is the mediator in the midst of source and end vehicle figured utilizing the Euclidean division. The scope of the commonplace zone circle is twice of the sending zone circle [8].

MANET security [9] [10] [12] [13] [14] [15] [16] is the key issue these days to handle in light of the way that different noxious ways are going into the system to make aggravations and lessening the structure execution. In this paper, we have discussed and relied upon to locate a practical organizing way and trade the information by scrambling it with the Session Key (SK) [11] to keep the information from getting got by an interloper. Position Based Secure Routing Protocol(PBSRP) a blend organizing convention, which combines the considerations of Message Ferry Route (MFR) [17] and B-MFR [17] to locate the ideal focus to hand-off the information. In the wake of discovering the ideal focus the standard thing is to check whether the inside is honest to goodness or not, for that station to station key association custom is utilized which does not utilize an untouchable for checking the middle point's authenticity yet it utilizes the affirmations for the vehicles to check whether the inside point is a veritable.

This method can be used by the assailants with the goal that there will be an opportunity to embrace the security system [18] [19].

2. LITERATURE REVIEW
In 2011, Irshad Ahmed Sumra et al. [20] present the Vehicular phenomenally assigned system Security R&d Ecosystem is examined. The R&d Ecosystem can be separated into four huge perspectives i.e. instructive examination, automobile producers, government powers, and end clients. In 2012, G.gowtham et al. [21] recommend that avanet is an adhoc form that uses moving cars as focuses in a structure to make a flexible system. VANET basically 100 to 300 meters of one another to interface and along these lines make a structure with a wide range. As cars drops out of the sign range and goes out of the structure and unmistakable autos takes after the same system and now adaptable structure is made. While trusting, if that middle point is discovered to be risky one, keep up an essential partition from correspondence with it. In their proposed work, as opposed to keeping up long records of focus point purposes of energy for focal trusted power, utilizing watchword generator convey a secret word and guard focus will legitimate them to the kid focuses. In 2012, Ganesh S. Khekare et al. [22] recommend that the unfathomable movement in the remote advances made a substitute kind of structures, for case, Vehicular Ad Hoc Networks (Vanets), which gives correspondence between vehicles themselves and in the midst of vehicles and base. Unmistakable new musings, for occasion, amazing urban gatherings and living labs are shown in the late years where Vanets has fundamental effect. In 2012, Khyati Choure et al. [23] recommend that in the present condition, in extemporized structure, the conduct of

focus focuses is not amazingly tireless. They don't work legitimate blue and alluring. They are not valuable and acting vainly. They demonstrate their preposterousness to present their advantages like transmission capacity to additional presence of battery; they are not put off to square the bundles sent by others for sending and transmit their own particular packs. In 2012, Ranbir Sinha et al. [24] present a considered improving the security in remote correspondence. A Computer Network is an interconnected amassing of overseeing toward oneself changing focuses, which utilize a satisfactorily depicted, by and large concurred game plan of models and traditions known as conventions, interface with each other really and permit asset offering ideally in a predicted and controllable way. Correspondence has a veritable effect on today's business. In 2013, Bhoi et al. [25] presents a substitute Position Based Secure Routing Protocol (PBSRP) which is a blend of Most Forward inside Radius (MFR) and Border Node based Most Forward inside Radius (B-MFR) coordinating customs. A security module is joined this convention by utilizing station to station key perception custom to keep the framework from particular strikes. It contains three stages: instatement stage, flawless focus point choice mastermind and secure information transport stage. Multiplication results shows PBSRP shows perfect results over MFR and B-MFR to the extent end to end postpone and group development degree when dangerous drivers are combined in the structure. In 2013, Li et al. [26] proposes a data scrambling course of action for urban VANET with high vehicle thickness and assorted hotspots. They increase honest to goodness controlling furthermore to additional the system assets the degree that this inevitable possible by presenting the thought about the Steiner tree issue. Reenactments are driven with NS-2.35 and MOVE. The diversion results demonstrate that our course of action performs better than RTDF plot in the execution of pack development delay. In 2013, Liya et al. [27] investigate the issue of perfect road side units (RSUs) circumstance in Vehicular Ad Hoc Network (VANET) on an expressway, which engages the VANET keep up a nice mix. Their goal is to find immaterial number of road side units, such that the vehicles could talk with RSUs. These road side units are related by wire. They add to a randomized figuring to send road side units in the VANET. It gives a nearby estimation to the perfect division to guarantee the information can be gone to RSUs from the accident site through the VANET. Diversions are coordinated to exhibit the execution of our proposed procedure. In 2013, Meng et al. [28] proposes an adaptable strategy in perspective of the mix of these two circumstances and a while later apply this system to Location-Aided Routing (LAR) tradition to keep the coordinating execution from corruption. In the flexible technique they use the Multiple Attribute Decision Making (MADM) to manufacture the control limit which can suit message transmission to the circumstances continuously. Theoretical examination and multiplication execution show that this technique can upgrade the pack transport extent (PDR) of LAR tradition effectively. In 2014, Correa et al. [29] work tries are concentrated, essentially, to analyze working settings in customs like AID, DBRS, and ADDHV for scattering messages. A benchmarking investigates technique that address challenges, for occurrence, system conveying the telecast tempest issue, which get a handle on the diffusing. The possible results of a course of action of estimations got in diverse vehicular improvement plans finish the exchange held. Examinations for answers in degree, deferral, rate of development, show, and pack accident help this activity and move the progress of a versatile reaction for changes in transporter thickness. In 2013, Amendola et al. [30] proposed a novel neighbor disclosure convention for asset limitation gadgets (RFID labels) running as per the deferral tolerant systems administration standard. The proposed convention is in light of the customary P-Persistent CSMA calculation, however with the expansion of the filter dissemination (siftPersistent) to diminish the crashes amid the reaction stage. Their proposition has been tried both in a test system and in a genuine testbed under the OpenBeacon structure. In 2014, Chasaki et al. [31] proposed a novel calculation to perform integration following in light of a space-effective Bloom channel information structure and the utilization of total marks. They exhibit recreation comes about on a genuine system follow that demonstrate the adequacy of their outline. Security based approaches are also suggested in [32], [33], [34] and [35].

3. PROPOSED METHOD

This paper presents an efficient scheme for malicious behavior identification and data security for dynamic nodes. For this we have presented an efficient framework malicious behavior identification and data security. The frame is designed in such a way that any node can be a part of the dynamic path as it is the possibility to allow the most in the same consideration. But allow to the several node may arise the possibilities of higher security risk. So in our approach we have provided two type of security in case of communication medium as the possibility of security breaches is mainly possible in this situation. There are two types of node arrangement here first is IN node and second is OUT node. The same category node may communicate with each other directly,but share their data with different level of key filtration applied by RSA and RC mechanism. For the out mode, there is an another condition by which the out node my available as the IN node but by accepting it from the other side. The file is then process by the above state along with the addition of extra hash code which will identify the malicious behavior. It is also clear from figure 1.

In the frst phase RSA algorithm is applied which is working as per the steps suggested in algorithm 1. The data is first prepared by the receiver node and then the cipher text is send to the requested node. The authorized node can view the data by applying the appropriate keys. Here there are there are three keys are needed namely public, private and modulas key. Based on the process the key length , number of keys, encryption and decryption time along with the size of the file is registered in the log details.

In the second phase data is prepared according to the RC mechanism the data is send to the authorized node. The node already receives one key from the requested node and it is process randomly. This mechanism is shown in figure 2. RC4 is a stream figure, symmetric key encryption calculation. The same calculation is utilized for both encryption and decoding. The information stream is just XORed with the arrangement of produced keys. The key stream does not rely on upon plaintext utilized by any means. A variable length key from 1 to 256 bit is utilized to instate a 256-bit state table. Vernam stream figure is the most broadly utilized stream figure in light of a variable key-size. It is famous because of its straightforwardness. It is frequently utilized as a part of document encryption items and secure correspondences, for example, inside SSL. The WEP (Wireless Equivalent Privacy) convention additionally utilized the RC4 calculation for classifiedness

Algorithm 1: RSA[36]

The Rivest-Shamir-Adleman (RSA) calculation is a standout amongst the most mainstream and secure open key encryption routines. The calculation reckons by the way that there is no proficient approach to component huge (100-200 digit) numbers.

Utilizing an encryption key (e,n), the calculation is as per the following:

1. Represent the message as a number somewhere around 0 and (n-1). Huge messages can be separated into various pieces. Every square would then be spoken to by a whole number in the same reach.
2. Encrypt the message by raising it to the eth power modulo n. The outcome is a ciphertext message C.
3. To unscramble ciphertext message C, raise it to another force d modulo n
4. The encryption key (e,n) is made open. The unscrambling key (d,n) is kept private by the client.

The most effective method to Determine Appropriate Values for e, d, and n

1. Choose two huge (100+ digit) prime numbers. Indicate these numbers as p and q.
2. Set n equivalent to p * q.
3. Choose any huge whole number, d, such that GCD(d, ((p-1) * (q-1))) = 1
4. Find e such that e * d = 1 (mod ((p-1) * (q-1)))

Algorithm 2: Rivest Cipher

1) Inputs: The arrangement of Input Files (IF1, IF2… … .IFn) from the full arrangement of solicitation by the customer client.
2) Output: Process File by the Server (PF1, PF2 … ..PFn).

do

cluster L[0,… , c - 1]

Number r of rounds

Pw = Odd((e – 2)2w)

Qw = Odd((ø – 1)2w)

Yield:

w-bit round keys S[0,… , 2r + 3]

Strategy:

S[0] = Pw

for i = 1 to (2r + 3) do

S[i] = S[i _ 1] + Qw

A = B = i = j = 0

v = 3 x max{c, 2r + 4}

for s = 1 to v do

{

A = S[i] = (S[i] + A + B) <<< 3

B = L[j] = (L[j] + A + B) <<< (A + B)

i = (i + 1) mod (2r + 4)

j = (j + 1) mod c

}

End;

Now we add the inherent hashing value, known as a polynomial hash, is not better than other hashing capacities in any capacity with the exception of straightforwardness. On the off chance that this basic hash capacity were utilized as a part of a hash table, it would be to a great degree simple for an opposing nodes to supply information that causes huge quantities of impacts. As a one application where this sort of polynomial hashing is conceivably helpful is in different string coordinating, which requires in moving hash esteem and malicious behavior detection. On the other hand, this is still powerless against adversarial information, which is the reason other, more thorough moving hash capacities or string coordinating calculations are by and large favored.

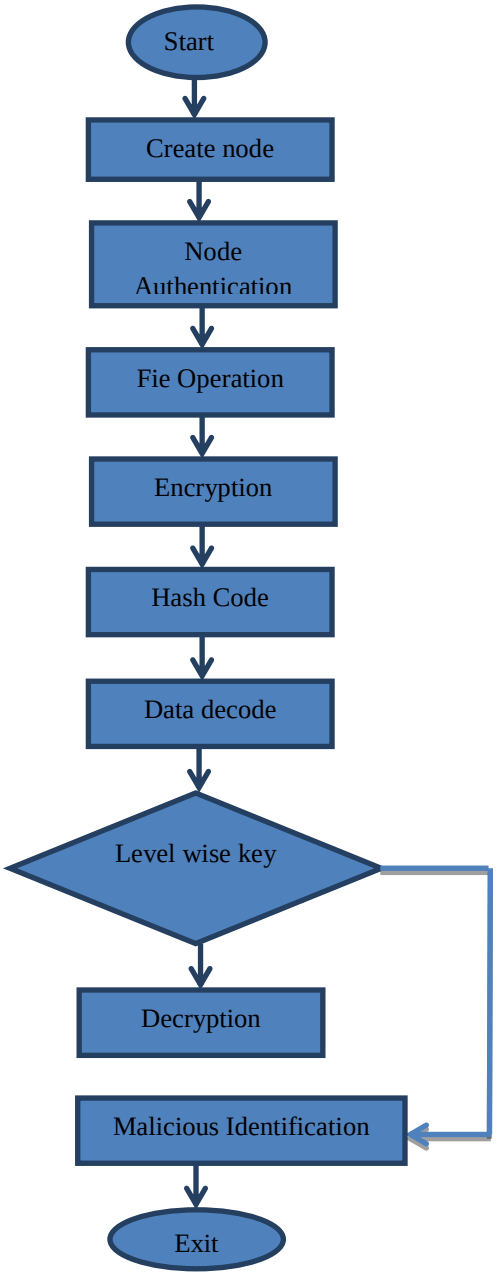

Figure 1: Flowchart

4. RESULT ANALYSIS

In this section results are presented by or method which shows the effectiveness of our approach. The node details are shown in table 1. It is the status which is after the registration. The key variations are shown in figure 2. The malicious identification has been shown with time comparison in figure 3. Figure 4 shows the key length comparison. The size after encryption and decryption is shown in figure 5. By these results we can say that this method is efficient in protecting data in case of dynamic nodes as well as it p[perform better in malicious behavior detection and it is compared with the time difference. So the communication path along with data terminal and exchanges may be secure.

Table 1: Node Details

Info					
Node name	**ID**	**TCP**	**IP**	**key**	**Node status**
Node1	ID1	80	192.168.1.101	iS3Rc1f6	IN
Node2	ID2	80	192.168.1.101	xH2Ub1u1	IN
Node3	ID3	80	192.168.1.101	kG2Wc7e9	IN
Node4	ID4	80	192.168.1.101	pG9Hq3e4	OUT
Node5	ID5	80	192.168.1.101	eB6Na6t6	OUT
Node6	ID6	80	192.168.1.101	zU4Bq3l3	OUT

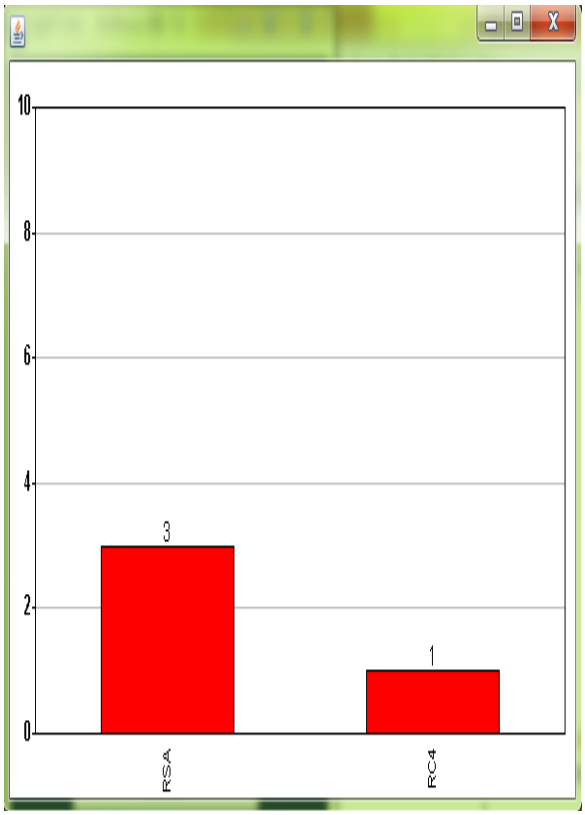

Figure 2: RSA and RC Keys

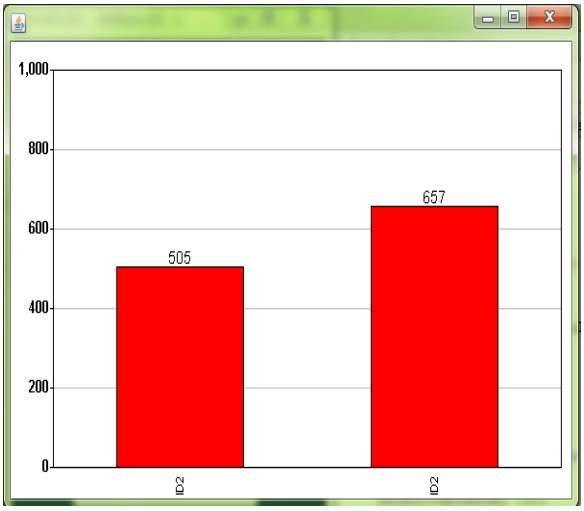

Figure 3: Malicious identification

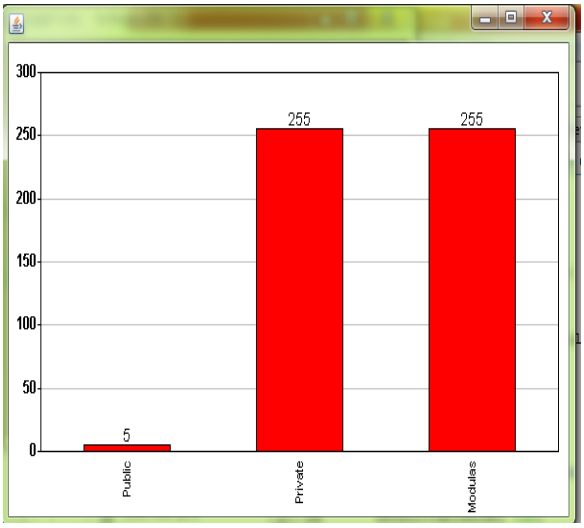

Figure 4: Key Length Comparison

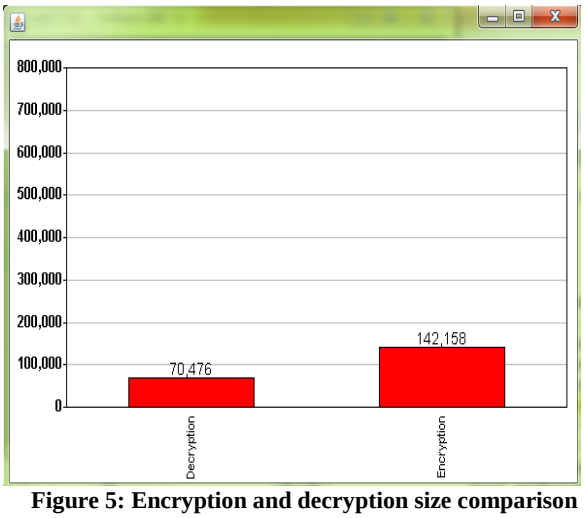

Figure 5: Encryption and decryption size comparison

5. CONCLUSIONS

Based on our study and examination on MANET security demonstrates different security breaches. Although there is a few explorations work is as of now in advancement and several other work is going in the full swing. However, the exploration has several vacuums in information security and assault recognition is still the range of future examination. So in this paper we have presented RSA and Rivest Cipher based

security mechanism to improve the data security as well as by the polynomial hash code malicious behavior is identified properly and timely.

6. REFERENCES

[1] Zhang, Y.; Lazos, L.; Kozma, W., "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks," Mobile Computing, IEEE Transactions on , vol.PP, no.99, pp.1,1.

[2] G. Acs, L. Buttyan, and L. Dora. Misbehaving router detection in link-state routing for wireless mesh networks. InProc. of WoWMoM, pages 1–6, 2010.

[3] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens. ODSBR: An on-demand secure byzantine resilient routing protocol for wireless ad hoc networks. ACM Transactions on Information System Security, 10(4):11–35, 2008.

[4] K. Balakrishnan, J. Deng, and P. K. Varshney. Twoack: Preventing selfishness in mobile ad hoc networks. InProc. of WCNC, 2005.

[5] S. Buchegger and J.-Y. L. Boudec. Self-policing mobile ad-hoc networks by reputation systems.IEEE Comm. Magazine, pages 101–107, 2005.

[6] K.V.Kulhalli, Prajakta Rane, "On Demand Multipath Routing Algorithm for Adhoc Wireless Networks ", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-14, March-2014, pp.357-363.

[7] Aruna Rao S.L, K.V.N.Sunitha, "Secure Geographical routing in MANET using the Adaptive Position Update ", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-16, September-2014, pp.785-794.

[8] Kambalimath, Mahantesh G., S. K. Mahabaleshwar, and S. S. Manvi. "Reliable Data Delivery in Vehicular Ad Hoc Networks." In Broadband and Wireless Computing, Communication and Applications (BWCCA), 2013 Eighth International Conference on, pp. 316-322. IEEE, 2013.

[9] T. Leinmuller, E. Schoch, and C. Maihofer, "Security Requirements and Solution Concepts in Vehicular Ad Hoc Networks," IEEE 4th Annual Conference on Wireless on Demand Network Systems and Services, pp. 84-91, 2007.

[10] Ma'en Saleh, Ahmad Aljaafreh and Naeem Al-Oudat , " Hierarchal Scheduling Algorithm for Congestion Traffi Control Using Multi-Agent Systems", International Journal of Advanced Computer Research (IJACR), Volume-4, Issue-17, December-2014 ,pp.915-921.

[11] C. Langley, R. Lucas, and H. Fu, "Key Management in Vehicular Ad-Hoc Networks," IEEE International Conference on Electro/Information Technology, pp.223-226, 18-20 May 2008.

[12] M. Burmester, E. Magkos, and V. Chrissikopoulos, "Strengthening Privacy Protection in VANETs," IEEE International Conference on Wireless & Mobile Computing, Networking & Communication, pp. 508-513, 2008.

[13] Nath, Asoke, et al. "Multi Way Feedback Encryption Standard Ver-2 (MWFES-2)." International Journal of Advanced Computer Research (IJACR) 3.1 (2013).

[14] F. Schaub, Z. Ma, and F. Kargl, "Privacy Requirements in Vehicular Communication Systems," IEEE International Conference on Computational Science and Engineering, pp. 139-145, 2009.

[15] F. Sabahi, "The Security of Vehicular Adhoc Networks," IEEE Third International Conference on Computational Intelligence, Communication Systems and Networks, pp. 338-342, 2011.

[16] J. M. de Fuentes, A. I. González-Tablas, and A. Ribagorda, "Overview of security issues in Vehicular Ad-hoc Networks", IGI Global, 2011.

[17] R.S. Raw, and D.K. Lobiyal, "B-MFR routing protocol for vehicular ad hoc networks," Networking and Information Technology (ICNIT), 2010 International Conference on, pp.420-423, 11-12 June 2010.

[18] Namrata Shukla, " Data Mining based Result Analysis of Document Fraud Detection " , International Journal of Advanced Technology and Engineering Exploration (IJATEE), Volume-1, Issue-1, December-2014 ,pp.21-25.

[19] Namrata Shukla, Shweta Pandey, " Document Fraud Detection with the help of Data Mining and Secure Substitution Method with Frequency Analysis " , International Journal of Advanced Computer Research (IJACR), Volume-2, Issue-4, June-2012 ,pp.149-156.

[20] Irshad Ahmed Sumra, Halabi Hasbullah and Jamalul-lail Ab Manan, "VANET Security Research and Development Ecosystem",IEEE 2011.

[21] G.Gowtham, E.Samlinson, "A Secured Trust Creation In V Anet Environment Using Random Password Generator",International Conference on Computing, Electronics and Electrical Technologies [ICCEET],2012.

[22] Ganesh S. Khekare, Apeksha V. Sakhare, "Intelligent Traffic System for VANET: A Survey", International Journal of Advanced Computer Research (IJACR), Volume-2, Number-4, Issue-6, December-2012.

[23] Khyati Choure, Sanjay Sharma, "Identification of node behavior for Mobile Ad-hoc Network", International Journal of Advanced Computer Research (IJACR), Volume-2 Number-4, Issue-6, December-2012.

[24] Ranbir Sinha, Nishant Behar, Devendra Singh," Secure Handshake in Wi-Fi Connection (A Secure and Enhanced Communication Protocol)", International Journal of Advanced Computer Research (IJACR) Volume 2, Number 1, March 2012.

[25] Bhoi, Sourav Kumar, and Pabitra Mohan Khilar. "A secure routing protocol for vehicular Ad Hoc network to provide ITS services." In Communications and Signal Processing (ICCSP), 2013 International Conference on, pp. 1170-1174. IEEE, 2013.

[26] Li, Y., J. Yang, and S. L. Wu. "A Steiner tree based information dissemination for urban vehicular Ad Hoc networks." In Computational Problem-solving (ICCP), 2013 International Conference on, pp. 113-117. IEEE, 2013.

[27] Liya, Xu, Huang Chuanhe, Li Peng, and Zhu Junyu. "A Randomized Algorithm for Roadside Units Placement in Vehicular Ad Hoc Network." In Mobile Ad-hoc and

Sensor Networks (MSN), 2013 IEEE Ninth International Conference on, pp. 193-197. IEEE, 2013.

[28] Meng, Jia, Hao Wu, Hengliang Tang, and Xingyu Qian. "An Adaptive Strategy for Location-Aided Routing Protocol in Vehicular Ad Hoc Networks." In Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on, pp. 405-410. IEEE, 2013.

[29] Correa, Claudio, Jo Ueyama, Rodolfo Ipolito Meneguette, and Leandro Aparecido Villas. "VANets: An Exploratory Evaluation in Vehicular Ad Hoc Network for Urban Environment." In Network Computing and Applications (NCA), 2014 IEEE 13th International Symposium on, pp. 45-49. IEEE, 2014.

[30] Amendola, Danilo, Floriano De Rango, Khalil Massri, and Andrea Vitaletti. "Neighbor discovery in delay tolerant networking using resource-constraint devices." In Wireless Days (WD), 2013 IFIP, pp. 1-3. IEEE, 2013.

[31] Chasaki, Danai. "Identifying malicious behavior in MANET through data path information." In Computing, Networking and Communications (ICNC), 2014 International Conference on, pp. 567-572. IEEE, 2014.

[32] Ashutosh Kumar Dubey, Animesh Kumar Dubey Mayank Namdev, Shiv Shakti Shrivastava ,"Cloud-User Security Based on RSA and MD5 Algorithm for Resource Attestation and Sharing in Java Environment",Conseg 2012, Published by IEEE.

[33] Li, Wenjia, and Anupam Joshi. "Security issues in mobile ad hoc networks-a survey." Department of Computer Science and Electrical Engineering, University of Maryland, Baltimore County (2008): 1-23.

[34] Sirwan Geramiparvar and Nasser Modiri, " Security as a Serious Challenge for E-Banking: a Review of Emmental Malware " , International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-18, March-2015 ,pp.62-67.

[35] Ketki P. Kshirsagar, " Key Frame Selection for One-Two Hand Gesture Recognition with HMM " , International Journal of Advanced Computer Research (IJACR), Volume-5, Issue-19, June-2015 ,pp.192-197.

[36] Wuling Ren; Zhiqian Miao, "A Hybrid Encryption Algorithm Based on DES and RSA in Bluetooth Communication," Modeling, Simulation and Visualization Methods (WMSVM),Second International Conference on , vol., no., pp.221,225, 15-16 May 2010.