Volume 6, Issue 3, March 2016 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Node Malicious Behavior Recognizing and Protecting in MANET

[1]Rajesh Solanki, [2]Neha Thakur, [3]Yogesh Rai
[1, 2] M.Tech Student, Computer Science, SIST, Bhopal, India
[3] Asst. Prof., Computer Science, SIST, Bhopal, India

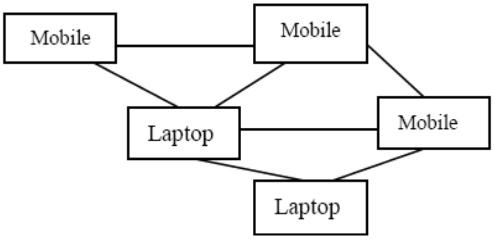
Abstract: Mobile ad hoc network (MANET) is a type of wireless ad hoc network, and is a self-configurable network devices connected by any mobile device of without wire. Every device in a MANET is liberated to move in any area. These types of network are occasionally self-controlled or controlled by any other network area. The data sharing and receiving in this environment is making this environment more folksy to use. The existing security-based solutions for the mobile ad hoc network environment are less secure as it is based on environment specific security but not releasing fully dynamically changes. security system is of more noteworthy concern. So in this paper A hash code is added to recongiges the Evil behavior detection by enumeration it timely. A cross breed encryption method based on Symmetric key Rivest Cipher (RC4) and Asymmetric cryptography Ron Rivest, Adi Shamir, and Leonard Adleman(RSA) is applied on the data for protecting it. The results also prove the effectiveness of this approach.

Keywords: Security, Attack, MANET, Malicious Node, Data sharing and gathering.

I. INTRODUCTION

The network devices to be available anytime and anywhere. It is not possible to get wired network link between the two ubiquitous devices every time and everywhere. Because of the advance communication system mobile ad hoc network (MANET) is a trending platform for the current research. This system model presupposes that middle hubs are ready to convey movement other than their own. At the point when impromptu systems are sent in unfriendly situations (strategic systems), or comprise of hubs that fit in with different autonomous substances, a convention agreeable conduct can't be accepted. Unattended gadgets can get to be bargained and drop travel activity keeping in mind the end goal to debase the system execution. Additionally, new clients might misconfigure their gadgets to reject sending activity keeping in mind the end goal to save vitality. This kind of conduct is normally termed node misconduct. MANET can provide information and services all time and everywhere at any geographic position. It can be very easily deploy at any place and time as it does not require any well established infrastructure. Because of these magnificent distinctiveness MANET has many applications. In adverse geographic conditions and locations MANET can establish distributed network system without any base stations. MANET has no central administrator or infrastructure. Due to this flexibility in the implementation of MANET it can be used in during natural calamities such as earthquake or flood like situations. It is used during emergency services, military or police operations. It plays important role in setting ad-hoc conferencing.

This paper concentrates on and talks about the arrangement for trustworthy data transport considering the adaptability of the vehicles as a genuine concern. Proposed arrangement recognizes the sending zone and expected zone. The vehicles with most noteworthy pace for pass on the data divide the sending zone, with a yearning of minimizing the deferral. Later in the typical zone of the end vehicle the data groups are broadcasted until they accomplish the end vehicle. Sending zone and expected zones are circles, the compass for sending circle is the partition amidst source and end vehicle figured using the Euclidean division. The range of the typical zone circle is twice of the sending zone circle. These networks are independent of any fixed infrastructure or central entity like cellular networks which requires fixed infrastructure to operate.



MANET security is the essential issue nowadays to handle in light of the fact that various poisonous drivers are going into the framework to make aggravations and diminishing the framework execution. In this paper, PBSRP coordinating tradition is expected to find a viable coordinating way and exchange the data by scrambling it with the Session Key (SK) to keep the data from getting got by an intruder. PBSRP is a mixture coordinating tradition which consolidates the thoughts of MFR [15] and B-MFR [15] to find the perfect center to hand-off the data. In the wake of finding the perfect center the standard thing is to check whether the center is genuine or not, for that station to station key organization tradition is used which does not uses an untouchable for checking the center point's legitimacy yet it uses the confirmations for the vehicles to check whether the center point is a veritable.

II. LITERATURE REVIEW

In 2012, Ranbir Sinha et al. [18] present a thought of enhancing the security in remote correspondence. A Computer Network is an interconnected assembling of administering toward oneself transforming centers, which use an adequately portrayed, generally agreed arrangement of models and conventions known as traditions, interface with one another genuinely and license resource offering in a perfect world in a foreseen and controllable way. Correspondence has a genuine impact on today's business. It is fancied to relate data with high security. These days remote correspondence has transformed into a significant sign of correspondence in all parts of regular life. The basic role behind this reputation other than everything else like the rate of correspondence and insignificant exertion is the solace of directing and dealing with data trade. However this correspondence is diminished by the untrustworthiness of correspondence.

In 2012, G.gowtham et al. [19] prescribe that avanet is an adhoc compose that uses moving automobiles as centers in a framework to make a versatile framework. VANET grants automobiles pretty much 100 to 300 meters of each other to interface and in this way make a framework with a wide range. As automobiles drops out of the sign range and goes out of the framework and distinctive cars takes after the same framework and now flexible framework is made. Here the correspondence between the center points happens in a secured way by using security computations like TESLA and Ecdsa. VANET uses a gear called trusted stage module to give a secured correspondence between the centers. For a secured correspondence between the centers, a center must trust the talking center before correspondence with it and in case it is found honest to goodness then talk with it. While trusting, if that center point is found to be dangerous one, keep up a vital separation from correspondence with it. In their proposed work, instead of keeping up long records of center point purposes of enthusiasm for central trusted force, using watchword generator deliver a mystery word and gatekeeper center will proper them to the child centers.

In 2012, Ganesh S. Khekare et al. [20] suggest that the boundless progression in the remote advances created an alternate sort of frameworks, for instance, Vehicular Ad Hoc Networks (Vanets), which gives correspondence between vehicles themselves and amidst vehicles and base. Distinctive new thoughts, for instance, splendid urban groups and living labs are displayed in the late years where Vanets has basic impact. A review of distinctive Intelligent Traffic Systems (ITS) open and diverse directing traditions in regards to our proposed arrangement is completed in this paper. They displays an alternate arrangement contain an insightful city framework that transmit information about movement conditions that will help the driver to take fitting decisions. Their proposed arrangement contain an advised message module made out of Intelligent Traffic Lights (Itls) which offers information to the driver about rhythmic movement action conditions.

In 2012, Khyati Choure et al. [21] suggest that in the current circumstance, in improvised framework, the behavior of center points is not amazingly relentless. They don't work honest to goodness and attractive. They are not useful and acting vainly. They show their silliness to confer their benefits like transmission ability to extra existence of battery; they are not postpone to square the packages sent by others for sending and transmit their own specific packs. On account of higher Mobility of the assorted centers makes the circumstances a great deal more jumbled. Distinctive directing traditions especially for these conditions have been created in the midst of the most recent few years, to find propelled courses from a source to some end. In the meantime it is still hard to know the genuine briefest path without aggressors or frightful center points. Extraordinarily delegated framework encounter the evil impacts of the piece of issues i.e. blockage, Throughput, delay, security, arrange overhead. Package movement degree is the issues of ceaseless examination. Purpose behind center point dissatisfaction may be either basic frustration of center associations or it may be a result of show of an attacker or awful center point which may degenerate execution of framework slowly or drastically, which furthermore need to perceive or chose. In this paper, they recognize the immense and horrendous centers. A propagation has been performed to accomplish better execution of changed AODV. Awesome result has been procured the extent that Throughout, Packet Delivery Ratio.

In 2013, Bhoi et al. [22] presents an alternate Position Based Secure Routing Protocol (PBSRP) which is a mixture of Most Forward inside Radius (MFR) and Border Node based Most Forward inside Radius (B-MFR) directing traditions. A security module is incorporated this tradition by using station to station key comprehension tradition to keep the system from distinctive strikes. It contains three stages: instatement stage, perfect center point decision arrange and secure data transport stage. Proliferation results shows PBSRP shows ideal results over MFR and B-MFR as far as end to end delay and bundle movement extent when malignant drivers are consolidated in the framework.

In 2013, Li et al. [23] proposes an information scrambling arrangement for urban VANET with high vehicle thickness and diverse hotspots. They gain true blue controlling and also to extra the framework resources the degree that this eventual conceivable by introducing the thought of the Steiner tree issue. Reenactments are driven with NS-2.35 and MOVE. The amusement results show that our arrangement performs better than RTDF plot in the execution of pack movement delay.

In 2013, Liya et al. [24] explore the issue of ideal street side units (RSUs) situation in Vehicular Ad Hoc Network (VANET) on a thruway, which empowers the VANET keep up a decent integration. Their objective is to discover insignificant number of street side units, such that the vehicles could speak with RSUs. These street side units are associated by wire. They add to a randomized calculation to send street side units in the VANET. It gives a close estimation to the ideal separation to ensure the data can be gone to RSUs from the mischance site through the VANET. Recreations are directed to demonstrate the execution of our proposed technique.

In 2013, Meng et al. [25] proposes a versatile technique in view of the blend of these two circumstances and afterward apply this methodology to Location-Aided Routing (LAR) convention to keep the directing execution from debasement. In the versatile procedure they utilize the Multiple Attribute Decision Making (MADM) to build the control capacity which can suit message transmission to the circumstances progressively. Hypothetical examination and reproduction execution demonstrate that this method can enhance the bundle conveyance proportion (PDR) of LAR convention successfully.

In 2014, Correa et al. [26] work tries are concentrated, basically, to examine working settings in traditions like AID, DBRS, and ADDHV for dissipating messages. A benchmarking explores methodology that address challenges, for instance, framework distributing the broadcast storm issue, which grasp the diffusing. The eventual outcomes of an arrangement of estimations got in different vehicular development arrangements complete the trade held. Examinations for answers in degree, delay, rate of movement, broadcast, and pack mishap help this action and move the headway of an adaptable response for changes in transporter thickness.

In 2014, Kiran Penna, et al. [27] proposed a generated different scenarios with variable velocity ranges and simulated the VANET and also considered the effect of delay, jitter in his simulation and observed that the proposed approach is robust and a feasible solution to the problem of Active Position detection.

III. 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. use one cryptographic algorithm RSA and sequence number calculation to eliminate the black hole node. Initially, the two large prime numbers has been taken and calculate the d and e value. The RREQ is considered as M. The RREQ is encrypted at the sender side and it forwards the RREQ to the neighbor's node. If the node knows key value then the node can able to decrypt the RREQ and it generates RREP to the source. After receiving the RREP in source, it computes the threshold_diff in which the RREP come from legitimate node or malicious node. Base on the threshold_diff, it sends the packet from source to destination. If the difference of sequence value is below the threshold_value, then the node is considered as legitimate node. Suppose, if the difference of Sequence number is greater than the threshold_value, then the node is considered as malicious node. 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 RC4 and RSA 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 first 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 RC4 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. The proposed algorithm is described as follows;

```
Step 1: RSA
Select any two prime numbers namely p and q (p! =q)
Calculate the followings
n=p*q
Ø (n) = (p-1)*(q-1)
gcd (e, n)=1 and find e
(d*e)% Ø (n) =1 and find d
Step 2:
M= RREQ
Step 3:
To encrypt the RREQ by using following
For i =0 till i<e
```

$C=C*M \bmod n$ Where $C=1$

Step 4:

Forward the RREQ to neighbor's node.

Step 5:

If the RREQ is received by the legitimate node, then decrypt the RREQ by using following

(i). Decrypt RREQ using the followings,

For $i=0$ till $i<d$

$M = M*C \bmod n$

Step 6:

Generate RREP based on RREQ

Step 7:

Forward RREP to source node

Step 8:

If RREQ is received by a black hole then decrypt as in Step 5,

Step 9:

Generate RREP

Step 10:

Forward RREP to source node

Step 11:

Check RREP at source on receiving RREP. This is done as follows:

(i). Decrypt the received RREP as in step 5.

(ii). If the RREP has come from a legitimate node, then RREP will be decrypted correctly. Set BHI (Black hole Indicator) to 0 to indicate that RREP has come from a legitimate node.

(iii). Else, the RREP has come from a black hole. Then Set BHI to 1

Step 12: Compute the Threshold_diff by using the following formula:

Threshold_diff = Current Sequence number – Previously received sequence number

If the difference is below the threshold value then the packet is forwarded Else if the difference is above the threshold_diff, then the value of threshold_diff is incremented and the packet is dropped.

Step 2: RC4

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;
```

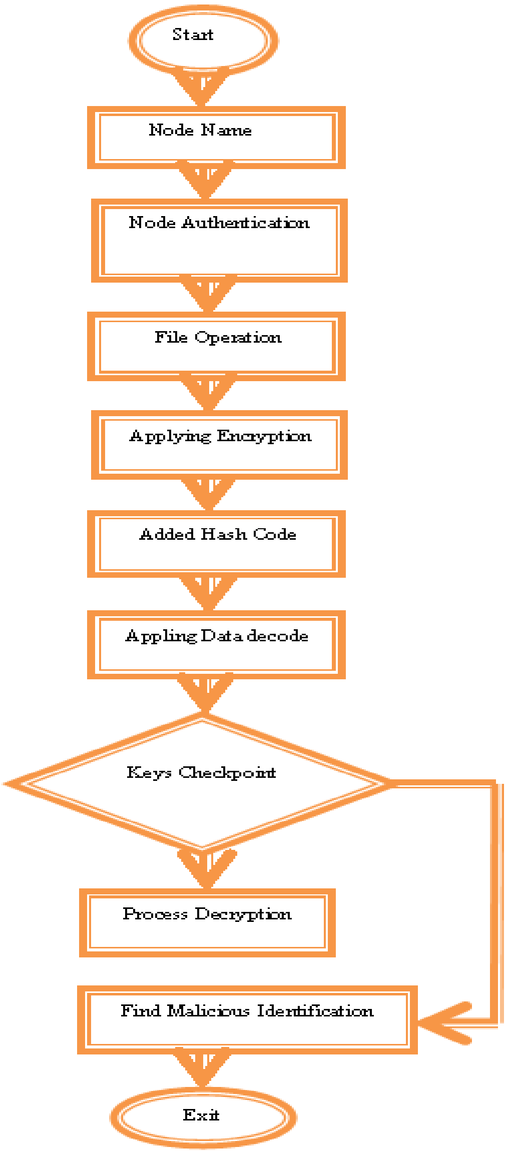


Figure 1. Flowchart

Now we add the inherent hashing values 0 and 1, 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.

Table: Identify Malicious Node Behavior

ID	Key Distribution	Periodically Updation Information of Node	Updation Time	Node Behavior	Attack	Security
ID1	PrID1, PuID1 ModID1	ID1(current status, source IP address) to all Node	30ms	T/F	Dos attack	RSA& RC
ID2	PrID2, PuID2 ModID2	ID2(current status, source IP address) to all Node	35ms	T/F	Bogs info attack	RSA& RC
ID3	PrID3, PuID3 ModID3	ID3(current status, source IP address) to all Node	38ms	T/F	Alteration attack	RSA& RC
ID4	PrID4, PuID4 ModID4	ID4(current status, source IP address) to all Node	40ms	T/F	Integrity attack	RSA& RC
ID5	PrID5, PuID5 ModID5	ID5(current status, source IP address) to all Node	45ms	T/F	Sybil attack	RSA& RC
ID6	PrID6, PuID6 ModID6	ID6(current status, source IP address) to all Node	50ms	T/F	Reply attack	RSA& RC

Node registration is successfully performed and the node IDs should allow with the pass key that is generated randomly. IDs are sharing data with key Distribution (Public, private, and modulas keys).After that checking periodically updating Information of node the node ID current status and source IP address to all nodes. Updating time will be given to the communication node IDs, in the meantime node id not response then the data will not be shared. If node behavior False (intruder node ID) means data is attacked, so the node ID will change the send data or remove the send data. If the Node behavior is True (genuine ID) then the data will share with different level of key filtration applied by RSA and RC mechanism.

IV. 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 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.

Info					
nodename	**ID**	**TCP**	**IP**	**Key**	**nodestatus**
Node1	ID1	80	192.168.1.15	nZ2Vf9o3	IN
Node2	ID2	80	192.168.1.15	jQ9Xp2l4	IN
Node3	ID3	80	192.168.1.15	rI3Vp9k0	OUT
Node4	ID4	80	192.168.1.15	nH2Yp2t0	OUT
Node5	ID5	80	192.168.1.15	aT1Or0f7	OUT
Node6	ID6	80	192.168.1.15	vB0Vp5c2	IN

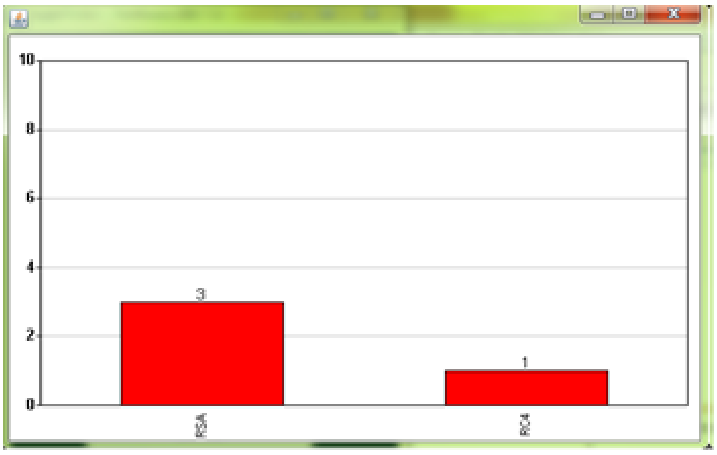


Figure 2: RSA and RC Keys

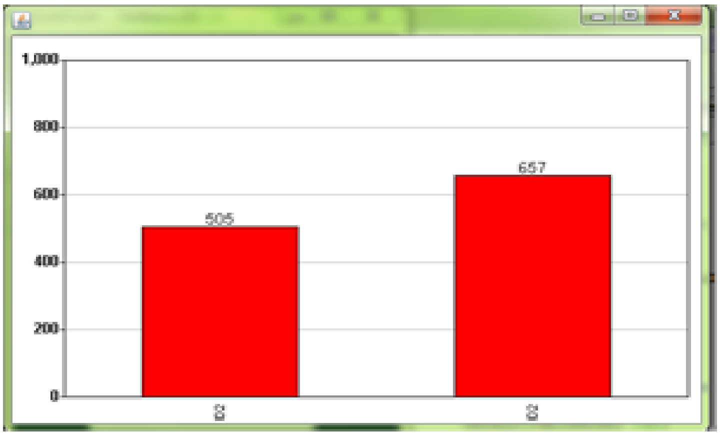


Figure 3: Malicious identification

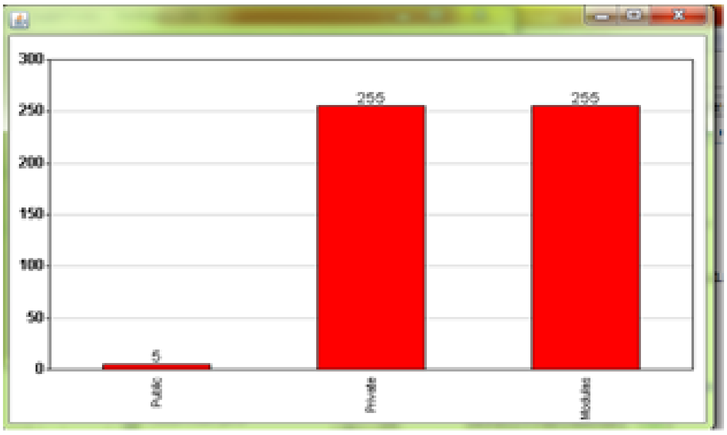


Figure 4: Key Length Comparison

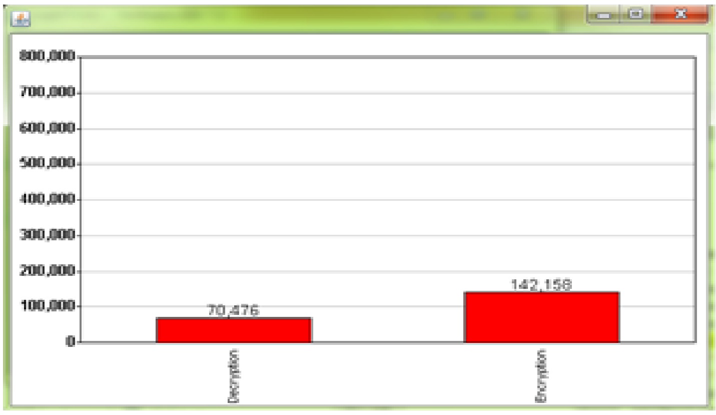


Figure 5: Encryption and decryption size compari

Our analysis based on the above study suggests the following direction:

Access control
Access control means guaranteeing that all nodes capacities as per the parts of benefits with which they have been approved in the system. For access control the approval needs to detail what is not can do in the system and what messages can be produced by it.

Anonymity
It implies that all the data that can be utilized to distinguish the manager or the current client of the hub ought to default be kept private and not be dispersed by the hub itself or the framework programming. This rule is nearly identified with security safeguarding, in which we ought to attempt to shield the security of the hubs from self-assertive revelation to some other elements.

Availability
The term availability means node should be able to provide services as and when required. The denial-of-service attack can affect the services provided by node. By repeatedly generating the route request malicious node exhaust the processing power of target and make the services provided by it unavailable.

Authentication
Authentication in MANET ensures that the communication node is genuine or not. It is fundamental for the correspondence members to demonstrate their characters as what they have asserted utilizing a few systems in order to guarantee the genuineness. In the event that there is not such a validation component, the enemy could mimic a kind hub and therefore become acquainted with classified assets, or even engender some fake messages to bother the ordinary system operations.

Confidentiality
Confidentiality means secrecy. Confidentiality can be gained only when the certain data can be accessed by authorized people. Other elements of the networks should not have privilege to access it.

Message Integrity
The received message should not be altered in the middle of the attack prior to the receiving. A message can be evacuated, replayed or overhauled by an enemy with noxious objective, which is viewed as malevolent modifying; in

actuality, if the message is lost or its substance is changed because of some kind disappointments, which may be transmission mistakes in correspondence or equipment blunders, for example, hard plate disappointment, then it is ordered as unintentional adjusting.

Message Non-Repudiation

Nonrepudiation guarantees that the sender and the collector of a message can't deny that they have ever sent or gotten such a message. This is valuable particularly when we have to segregate if a hub with some strange conduct is traded off or not: if a node perceives that the message it has gotten is wrong, it can then utilize the off base message as a confirmation to tell different hubs that the hub conveying the ill-advised message ought to have been bargained.

Entity authentication

The validation of the entity should be checked that the node should not pretend as the authentic node.

Denial of Service attack (DoS)

It assault, an assailant endeavors to keep genuine clients from getting to data or administrations. A disavowal of administration (DoS) assault is an assault that stops up such a great amount of memory on the target framework that it can't serve its clients, or it causes the target framework to crash, reboot, on the other hand overall refuse any assistance to true blue clients. Nowadays, DoS assaults are extremely regular; for sure, pretty much every server is certain to experience such an assault sooner or later or an alternate. Refusal of Service can without much of a stretch be propelled and surge the system with spurious steering messages through a pernicious hub that gives inaccurate redesigning data by claiming to be a real change of directing data.

Scalability

Scalability is not directly related to security but it is very important issue that has a great impact on security services. An ad hoc network may consist of hundreds or even thousands of nodes. Security mechanisms should be scalable to handle such a large network.

Gray Hole Attack

Gray hole attack, initially malicious node behaves normally i.e. during route discovery. But, as soon as it starts receiving the data packets it begins dropping it. Sometimes attacker node behaves normally while forwarding the data packet, whereas sometimes it behaves maliciously by dropping the data packets.

Internal Black Hole Attack

Black hole attack, a malicious node will claim that it has freshest and shortest path to the destination without referring to the routing table. In this way attacker node will always reply to the route request and thus intercept the data packet and retain it.

V. CONCLUSION AND FUTURE SUGGESTIONS

Our study and analysis on MANET security shows the vulnerable to threats and that the solutions developed for standard networks are often unsuitable in this environment and the leaks in security. Although there is several research work is already in progress in this direction. But the research vacuum in data security and attack detection is still the area of future research. In our view a proper encryption decryption process not completely cure this problem. But making a standard detection technique will be a powerful tool in future to prevent this in the greater extent.

We have also presented attacks and misbehavior on data forwarding which have received relatively less attention in literature, we think securing data forwarding is a fertile field of research. In our discussion we have shown how this solution may accuse wrongly a well-behaving node, and how it is unable to detect what we have called cooperative misbehavior. Preventive measures fail have been presented. We think securing ad hoc networks is a great challenge that includes many opened problems of research, and receives more and more attention among ad hoc networks community.

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 the polynomial hash code malicious behavior is identified properly and timely, RSA and Rivest Cipher based security mechanism to improve the data security.

For our future research, we plan to develop a suite of security mechanisms that not only protect security and conditional privacy, but also provide fast authorless authentication and privacy tracking with minimized secret storage and minimum cryptographic overhead.

REFERENCES

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

[2] 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.

[3] 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.

[4] 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.

[5] 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.

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

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] T. W. Chim, S. M. Yiu, L. C. K. Hui, and V. O. K. Li, “Security and Privacy Issues for Inter-vehicle Communications in VANETs,” IEEE Sensor, Mesh and Ad Hoc Communications and Networks Workshops, pp. 1-3, 2009.

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

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

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] Kiran Penna, Venkatesh Yalavarthi, Huirong Fu “Evaluation of Active Position Detection in Vehicular Ad Hoc Networks” 2014 International Joint Conference on Neural Networks (IJCNN)