PROBABILISTIC RANDOM RANGE TECHNIQUE FOR SECURING TEXT OVER MOBILE ADHOC NETWORK

Pritpal kaur[1], Er. Gaurav kumar[2]

[1]M.Tech, CSE, Global Institute of Management and Emerging Technology, Punjab, India
[2]Professor, CSE, Global Institute of Management and Emerging Technology, Punjab, India

---***---

ABSTRACT: *The MANET is infrastructure less and self-configured network due to which MANET is most favourable network for wireless transmission the MANET is better medium of communication that old method the transmission in MANET is fast and more efficient in case of long distance MANET is less expensive than old system. There are currently two variations of movable wireless networks communication and a smaller amount of networks. The infrastructure networks, also known as Cellular network, have permanent and energetic gateways. The various communication devices are evolved in MANET for efficient transmissions some fixed devices are used for better transmission are called base station. The security of data send by sender and receiver are done by encryption and decryption the various encryption and decryption technique are used for stopping the tempering of data the less energy consuming technique are used for encryption and decryption are used with less time consumption for efficient and fast transmission. In selective encryption only particular part of message is encrypted. Selective encryption works on some portion message it reduces time but the message is not fully secure in selective encryption technique .the probabilistically selective encryption.in proposed technique the uncertainty will be generated for encryption the percentage amount of encryption will be done by proposed technique which will increases security and it will perform better and fast while transmission .the proposed technique help in reducing encryption decryption time and enhances security in comparison to the selective encryption approach, since the encryption ratio is randomly decided and the encryption pattern is not pre-determined which enhances security of message while transmission.*

KEYWORDS: MANET, SSDE, PSRE .

I. INTRODUCTION

Wireless technologies such as Bluetooth or the 802.11 standards allow mobile devices to set up a Mobile Ad-hoc Network (MANET) by connecting energetically through the wireless medium without any centralised organization .MANETs propose several advantages over traditional networks including cheap communications costs, ease of establishment and fault tolerance. The set of connections of Infrastructure less system is known as Mobile Ad Network (MANET). A Mobile Ad-hoc Network (MANET) is a self-configuring set of connections of wireless and hence mobile devices that form a network talented of energetically altering topology.

II. ROUTING PROTOCOL

A. AD-HOC ON-DEMAND DISTANCE VECTOR (AODV)

AODV uses arrangement numbers and steering reference points from DSDV yet performs course disclosure utilizing on-request course asks for (RREQ); an indistinguishable procedure from the DSR convention. AODV is diverse to DSR in that it utilizes separate vector directing; this requires each hub in the course to keep up an impermanent steering table for the term of the correspondence. AODV has enhanced the DSR course ask for process utilizing a growing ring look system in view of augmenting time-to-live (TTL) to counteract unreasonable RREQ flooding. Hubs inside a dynamic course record the senders address, succession numbers and source/goal IP address inside their directing tables, this data is utilized by course answer (RREP) to build invert ways. AODV manages hub versatility utilizing succession numbers to distinguish and dispose of obsolete courses, this is consolidated with course mistake (RERR) messages which are sent when broken connections are identified, RERR parcels make a trip upstream to the source educating hubs to erase the broken connections and trigger new course revelation if elective courses are not accessible.

III. CLASSIFICATION OF ATTACKS

A. ATTACKS AT PHYSICAL LAYER

1. **Eavesdropping:** The fundamental focus of such assaults is to get to that mystery information which ought to stay private up and down the correspondence.
2. **Jamming**: The point of sticking is to make a check between two associating hubs by diminishing the radio signs to clamour proportion. An assailant can win this objective by creating another more grounded signal.

B. ATTACKS ON DATA LINK LAYER

1. Traffic Analysis: Traffic checking and examination is really not an assault, rather a device to plan such a one. An aggressor can get private data about the conveying hubs inside the system. For example, for to what extent two clients are in correspondence with each other, and also find their conveying functionalities. With the assistance of such particular data, it is less demanding for a malignant hub to pick how to assault a hub, pointing proficiency.

C. ATTACKS ON NETWORK LAYER

Different types of attacks are categorized as follows:

I. **Black hole Attack:** In this attack, the unauthorized node tries to stop the communication between nodes by declaring that it has a best way to the goal node. Once the node manages to put itself among communicating nodes, it can do anything with packets moving in the network.

3. **Wormhole Attack:** Wormhole Attack: In this assault, malevolent hub gets data toward one side in the system furthermore, pushes it toward another assailant hub. The wormhole is alluded to as tram that exists between two malignant hubs. Wormholes are utilized by the aggressors in the system to show their hub as more alluring with a specific end goal to course more information through them.

III SECURITY GOALS

1. Availability: It guarantees the accessibility of administrations, offered by the hubs, to its clients, and also ensure the survival of system gadgets if there should arise an occurrence of DOS assaults.

2. Integrity: Integrity ensures the ID of parcel when it is transmitted. It guarantees that parcels are not altered amid transmission.

3. Authentication: Authentication ensures that the conveying hubs and the wellspring of data are approved. An assailant can increase unlawful access to mystery data and assets and presumably meddle with the operation of different gatherings. Approval is ordinarily used to enable consents to various individuals.

4. Confidentiality: Confidentiality implies that some real messages are just congenial to those jumps that have been permitted to get to it. This ensures the security of mystery information.

5. Non-Repudiation: Non-Repudiation portrays the way that if a hub in MANET communicates something specific then it can't decline to the performed movement. This action is useful in revelation of egotistical hubs.

RELATED WORK

Ajay Kushwaha, Hari Ram Sharma et al[2016] The point of sticking is to make a check between two associating hops by diminishing the radio signs to noise proportion. An assailant can win this objective by creating another more grounded signal. **[1]**

Dilsher Singh et al [2015] because of its self-sorting out nature the Mobile Ad hoc Networks (MANETs) are effectively ready to give an incredible channel to correspondence anyplace, whenever without any brought together framework and have a gigantic potential in genuine applications like, in the military, safeguard and business fields.**[2]**

Rashika Indoria et al [2015] assessed that a remote impromptu system is a system where hubs can speak with each other without the help of framework. It can be set up effectively and rapidly with minimal effort. The system is called specially appointed on the grounds that every hub in the system is prepared to forward the information for different hubs thus the choice of which hubs exchange the information is made powerfully in view of the system network. **[3]**

Kumari, S.V. et al [2015] anticipated an improved Ant based Defense Mechanism for Selective Forwarding Attack in MANET. A SACK plan to transmit the safe affirmation is executed. A trust display is intended to distinguish assailants. **[4]**

Echchaachoui, A. et.al [2014] proposed a security answer for the Routing Protocol OLSR. The framework depends on awry and dynamic encryption. The principle reason behind the approach is to secure the activity against potential assaults without diminishing system exhibitions **[5]**

Haojie Shen et al [2014] proposed two layer choice plans for specific video encryption calculation which is contrasted and existing SEH264 calculation in which security and cryptographic security are accomplished,. The test comes about demonstrate that the proposed encryption calculation diminishes the computational multifaceted nature by half by and large. **[6]**

Yuefa Hu. et al [2012] proposed another specific encryption calculation which encodes one thousandth or less of video information yet with generally high security level. This calculation can be utilized for viably ensuring the video content. **[7]**

Ramdan, et al [2012] proposed a Skype customer application made particularly for video calling. Encryption is connected to video call information to keep it mystery. Its fundamental object is to actualize a particular encryption calculation in video calling, particularly by means of Skype. **[8]**

Yonglin et al [2011] display a probabilistic particular encryption calculation which uses the upsides of the probabilistic strategy that plans to procure extra vulnerability. **[9]**

Roy M et al [2011] proposed one particular video encryption calculation to manage the constant security necessities. One piece choice calculation to choose the higher serious bits to accomplish higher visual corruption is acquainted with accomplish higher visual debasement. In this paper, we have utilized AES encryption calculation for encryption. This upgrades the cryptographic security of the calculation which will be appropriate for constant information transmission application. **[10]**

Uma Parvathi, M. et al [2010] introduced a similar investigation of ordinarily utilized symmetric encryption calculations AES, DES, 3DES and Blowfish as far as power utilization. AES has a superior execution than other basic encryption calculations utilized. 3DES demonstrated poor execution comes about contrasted with other algorithms. **[11]**

PROPOSED METHODOLOGY

The point of propose approach a Probabilistically Selective Random Encryption (PSRE) algorithm, which utilizes the upsides of the probabilistic system, intending to acquire adequate instability. While transmission sending message from source to destination the proposed technique will display encryption ratio that how much data should be encrypted, It will identify that how many message should be encrypted instead of all message while transmission due to which the encryption process will faster in proposed technique. At that point, the sender utilizes a probabilistic capacity to pick the proposed deterministic measure of messages to deliver them. It shows that more vulnerability is incorporated to the PSRE algorithm in contrast with the SSDE, since the encryption proportion is arbitrarily chosen and the encryption design is not pre-decided. Also, this proposed PSRE algorithm is included the accompanying three stages:

1.The sender sending message SE will initially apply an arbitrary generator RNG to randomly get an encryption proportion err, which decides the rates of uncertain messages among all messages. Here, with a specific end goal to guarantee that enough information can be uncertain in order to give adequate security assurance, the produced encryption proportion ought to be higher than a pre-decided estimation of security prerequisite (SR implies that information correspondence is secure if there are SR or more percents of messages are encoded).

$$\boxed{\mathbf{SE} \xrightarrow[\mathbf{RNG}]{} \mathbf{eer} \mid \{\mathbf{err} \geq \mathbf{SR}\} \qquad (1)}$$

2. At that point the sender S will utilize an random probabilistic capacity RPF to produce an arbitrary encryption likelihood pi to decide whether one message Mi will be encoded or not.

$$\boxed{\mathbf{SE} \xrightarrow[\mathbf{PF}\ (\mathbf{M}_i)]{} \mathbf{Pi} \qquad (2)}$$

3. After find random probability the sender chooses the messages to encrypt for the above pre-decided encryption proportion er. For instance, once S discovers that the encryption probability pi is not exactly or equivalent to the encryption proportion err, it will encode the message Mi utilizing its secret key SK; generally, this message won't be changed in that way.

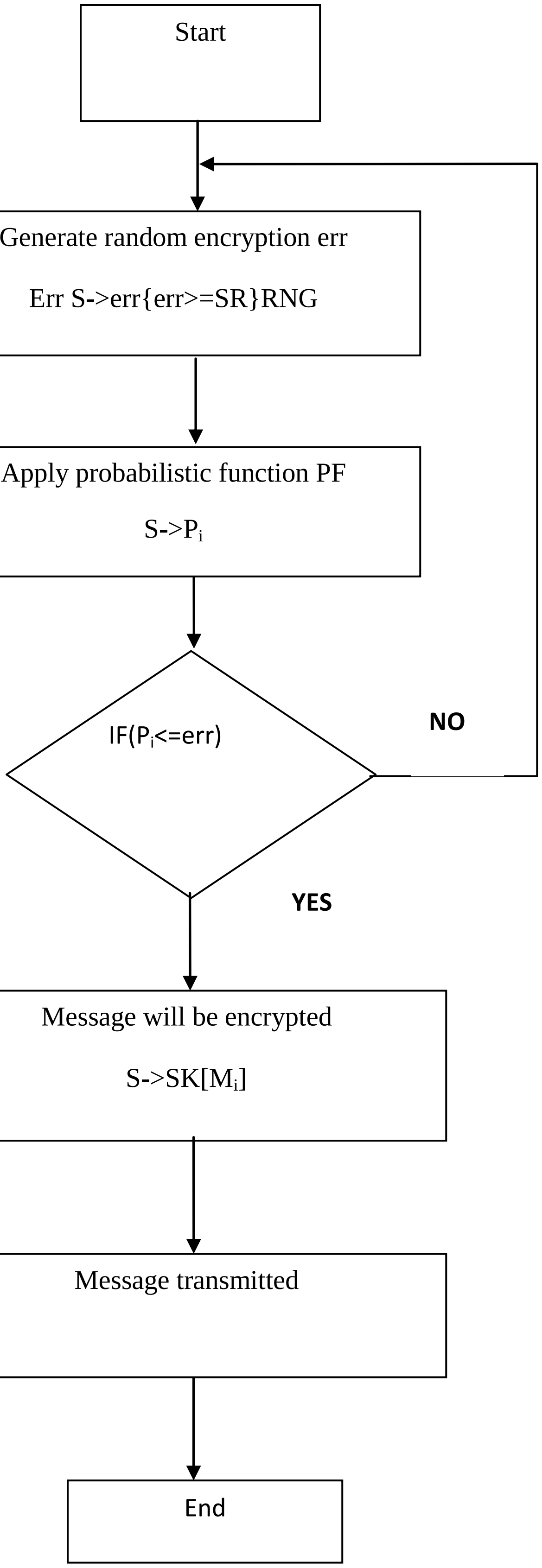
$$\boxed{\begin{array}{ll} .SE \rightarrow SK\,[M_i] & p_i \leq err \\ SE \rightarrow M_i & p_i > err \quad (3) \end{array}}$$

The probabilistic irregular encryption algorithm coordinates both the probabilistic technique and random selection of encrypted values, keeping in mind the end goal to build the vulnerability while sending message for transmission. The probabilistic encryption algorithm only takes portion of message for encryption on the basis of probability .The proposed techniques works better as compared to previous technique.

The Exchange of Selective Pattern

Once the sender of the conveying network exchanges the official exchange by methods for particular encryption, it will tell the comparing collector the encryption example of the communicated messages security. To start with, the sender will reduce the encryption process those probabilistic specifically change messages and show which messages have been encoded. In this way, it forms the encryption design in an example related message and after that sends it to the messages' collector. Therefore, the collector can utilize its comparing private key to encode the example message and consequently monitor the data of encoded messages. Through such an open key based strategy, the procedure of example data trade is kept secret just to the communicating network.

```
1: for time=1 to simulation time
2: for i=1: N, where N the number of nodes
    that located in the network
3: Generate random encryption err
    Within the range RNG
4: Apply probabilistic function PF ($M_i$) $P_i$
5: IF (Pi<=err)
6: Message will be encrypted S->SK [Mi]
7: else
8: Go to: step2
9: end if
10: end
```


Start
Generate random encryption err
Err S->err{err>=SR}RNG
Apply probabilistic function PF
S->P_i
IF(P_i<=err)
NO
YES
Message will be encrypted
S->SK[M_i]
Message transmitted
End

RESULT ANALYSIS

1Encryption time: The time taken by algorithm to encrypt text. The proposed probabilistic selective encryption algorithm integrates both the probabilistic method and random text selection method for encryption on the base of probability strategy, in order to increase the uncertainty in the process of message selection. The Fig 1 and Table 1 show that the encryption time taken by proposed algorithm is less as compared to compared to previous technique which means that proposed technology shows better performance as compared to previous technology. This shows that proposed technique is faster and more efficient than previous technique

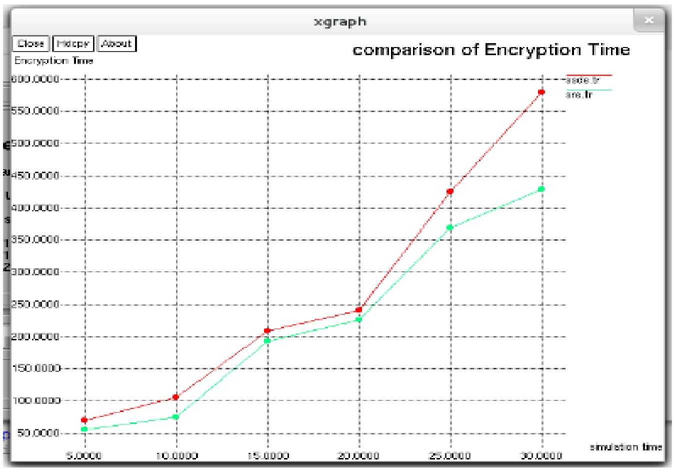


Fig1 Comparison of Encryption Time

Simulation time	PSRE	SSDE
5	55	70
10	75	105
15	193	209
20	226	241
25	369	425
30	429	580

Table 1 Comparison of Encryption Time

2 Encryption Saving Time: The Proposed technology work faster as compared to previous technology in proposed PSRE range of data is encrypted with maximum level of encryption required .The proposed technology encrypt random portion of data which is faster as compared to previous technique .The Fig 2 and Table 2 result shows that PSRE proposed technique is faster as compared to proposed technique .The proposed technique save time as compared to proposed technique.

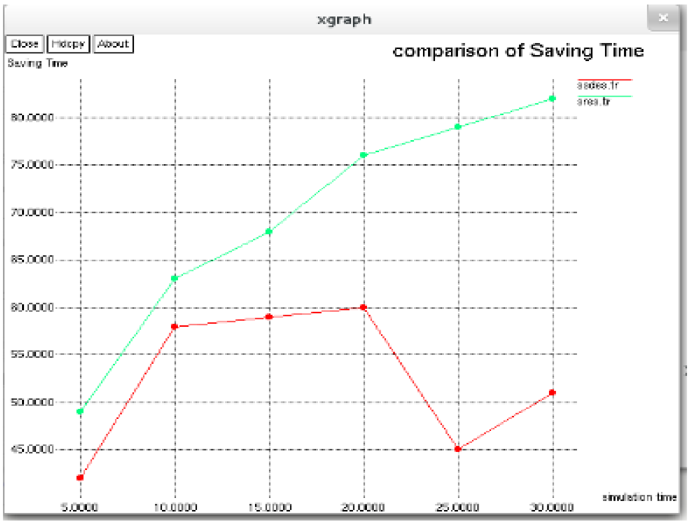


Fig 2 Comparison of Saving Time

Simulation time	PSRE	SSDE
5	49	42
10	63	58
15	68	59
20	76	60
25	79	45
30	82	51

Table 2 Comparison of Saving Time

3 Encryption proportion: The maximum data encryption means that maximum part of data is encrypted .The proposed technique encrypt maximum part of data encrypted as shown in Fig 3 and Table 3 the result of proposed technique is better that previous technique.

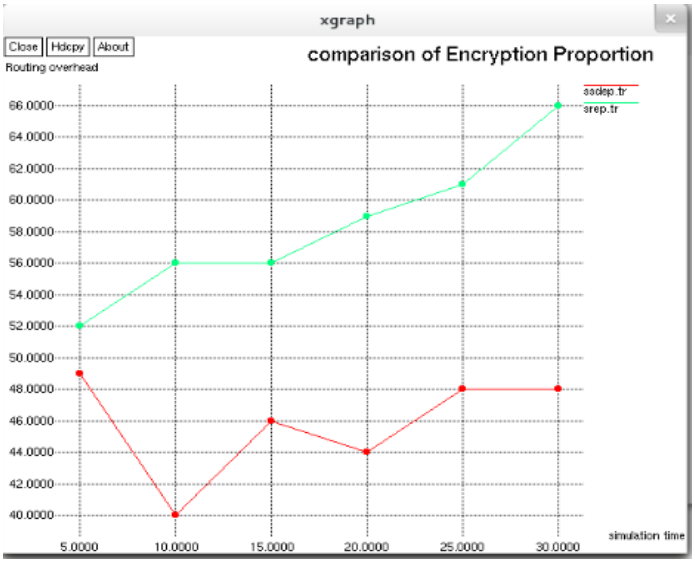


Fig 3Comparison of Encryption proportion

Simulation time	PSRE	SSDE
5	52	49
10	56	40
15	56	46
20	59	44
25	61	48
30	66	48

Table 3 Comparison of Encryption proportion

CONCLUSION

MANET provide various application for many problems in network encryption technique is provided for sending secure data in network .Network can be prevented or detected using cryptography methods. The security of data send by sender and receiver are done by encryption and decryption the various encryption and decryption technique are used for stopping the tempering of data .The less energy consuming technique are used for encryption and decryption are used with less time consumption for efficient and fast transmission. In selective encryption only particular part of message is encrypted. Selective encryption works on some portion message it reduces time but the message is not fully secure in selective encryption technique The encryption technique should be fast while transmission .The proposed technique work on random probabilistic technique which take the required portion of data for encryption instead of entire data due which the encryption process will be fast and it will reduce overhead time and provide more security while transmission.

REFERENCES

[1]Ajay Kushwaha, Hari Ram Sharma, Asha Ambhaikar," A Novel Selective Encryption Method for Securing Text over Mobile Ad hoc Network", 7th International Conference on Communication,Computing and Virtualization 2016[2016]

[2]Muhammad Kashif Nazir, Rameez U. Rehman, Atif Nazir, "A Novel Review on Security and Routing Protocols in MANET" Communications and Network, 2016, 8, 205-218[2016]

[3]Dilraj Singh, Dr. Amardeep Singh, "Multipath trust based framework for prevention of black hole attack in Manets" (JATIT & LLS), Vol.80. No.3, October 2015[2015]

[4]Rashika Indoria, Deepak Motwani, "An Approach of Detecting Cooperative Black Hole Attack in MANET using Modified TAODV Protocol" (IJCA),Vol.129. No.12, November2015[2015]

[5]kumara, S.V., Paramasivan, B., " Ant based Defense Mechanism for Selective Forwarding Attack in MANET", Data Engineering Workshops (ICDEW), 2015 31st IEEE International Conference, 2015, pp 92-97[2015]

[6] Echchaachoui, A., Choukri, A. ; Habbani, A. ; Elkoutbi, M., " Asymmetric and dynamic encryption for routing security in MANETs", Multimedia Computing and Systems (ICMCS), 2014 International Conference, 2014, pp 825-830.[2014]

[7]Haojie Shen, Li Zhuo ; Yingdi Zhao, "An efficient motion reference structure based selective encryption algorithm for H.264 videos",Information Security, IET (Volume:8 , Issue: 3), 2014, pp 199-206.[2014]

[8]Alex Hinds, Michael Ngulube, Shaoying Zhu, and Hussain Al-Aqrabi," A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)" International Journal of Information and Education Technology, Vol. 3, No. 1, February 2013[2013]

[9] Yuefa Hu, Xingjun Wang, "A novel selective encryption algorithm of MPEG2 streams", Consumer Electronics, Communications and Networks (CECNet), 2nd International Conference, 2012, pp 2315-2318.[2012]

[10]Ramdan, A.A. ; Munir, R., "Selective encryption algorithm implementation for video call on Skype client" TelecommunicationSystems, Services, and Applications (TSSA), 2012 7th International Conference on , 2012, pp. 120 - 124.[2012]

[11] Azzedine Boukerche, Lynda Mokda YonglinRen, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks," IEEE, 2011, pp. 1038- 1043.[2011]

[12]Roy, M. ; Pradhan, C., "Secured selective encryption algorithm for MPEG-2 video," Electronics Computer Technology (ICECT), 2011 3rd International Conference on Volume: 2, 2011, pp. 420 - 423.[2011]

[13]Umaparvathi, M., Varughese, D.K., "Evaluation of symmetric encryption algorithms for MANETs", Computational Intelligence and Computing Research (ICCIC), 2010 IEEE International Conference, 2010, pp 1-3.[2010]