Volume 4, Issue 6, June 2014 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

OOS Provisioning in Rural Wireless Mesh Network

Amrut R. Pawar*
SVERI's College of Engineering Pandharpur
Department of Computer Science &
Engineering, India

Amit R. Sarkar
SVERI's College of Engineering Pandharpur
Department of Computer Science &
Engineering, India

Abstract— Wireless Mesh Network (WMN) is a promising wireless network architecture having potential of last few miles connectivity. There has been considerable research work carried out on various issues like design, performance, security etc. in WMN. Due to increasing interest in WMN and use of smart devices with bandwidth hungry applications, WMN must be designed with objective of energy efficient communication. As networks are designed to meet quality of service (QoS) as per worst conditions, allows scope for tuning parameters to suit current environment/traffic conditions etc. towards goal of energy efficient communication. Quality of service provisioning is a challenging issue in rural WMNs because of limited bandwidths and security overhead from full encryption. Security is one of the most challenging aspects in internet and network applications domain. In this domain the major issue is to provide security to the data which is travelling on the communication link. Data encryption is the primary solution to protect the data confidentiality and integrity between any pair of node. Using symmetric key algorithms fast and efficient cryptosystems can be built as they have significant applications. For a wireless ad-hoc network with constraint computational resources, the cryptosystem based on symmetric key algorithms is extremely suitable for such an agile and dynamic environment along with other security strategies. The selective encryption algorithms are preferred by wireless networks because they are energy efficient for wireless devices. Probabilistic methodology and proposed algorithm enable a sender to include proper uncertainty in the process of message encryption so that only entrusted receiver can decrypt the cipher text and other unauthorized nodes have no knowledge of the transmitted messages on the whole. NS2 is used as testbed.

Keywords— WMNs, QoS provisioning, Energy efficiency, Selective encryption.

I. INTRODUCTION

Wireless mesh networks (WMNs) are a special case of ad hoc networks, which allow multiple hops, increase the coverage area, and have low implementation cost and support ubiquitous features for Internet access. WMNs comprising of mobile and static nodes connected wirelessly are emerging as a key technology for future generation of wireless networks. WMNs self-organize, self-configure and self heal themselves and can increase the coverage of conventional infrastructure-based wireless LANs and MANs without significant additional infrastructure deployments. Due to these unique features, WMNs are being used in many applications ranging from emergency response situations to wireless metropolitan area networks. Quality of Service (QoS) provisioning in WMNs is of utmost importance in order to support real time audio and video communications. However, QoS provisioning in highly mobile wireless networks such as WMNs is a very challenging problem compared to provisioning of QoS in wired IP networks.

The main reasons for this are unpredictable node mobility, wireless multi-hop communication, contention for wireless channel access, limited battery power and wireless range of mobile devices, as well as the absence of a central coordination authority in WMNs. There are many aspects wherein the QoS would be thought of, but here focus is on QoS provisioning in rural WMNs. In rural WMNs battery backup and the limited bandwidth are the main problems which oppose QoS provisioning [4]. Due to existing encryption techniques based on full message encryption there is security overhead, which increases the transmission time and hence results in less battery backup. A fundamental method of data protection in the area of information and network security is cryptography. It has been widely accepted as a traditional platform for achieving data confidentiality and integrity.

The application of cryptography is particularly prevalent today as it is exhaustively used today in homeland security, military communications, financial transactions and so on [6]. The method of data encryption and decryption are divided into symmetric encryption and asymmetric encryption [7]. However, a wireless ad-hoc network based on the features of wireless devices has special security and efficiency requirements for conventional cryptographic algorithms. As one of the mainstream cryptographic methods, symmetric key algorithms are widely used due to their efficiency and capability of data protection. Typically, a symmetric key cryptosystem employs a secret key for both encryption and decryption. This secret key is the only shared by sender and receiver and kept confidential to other irrelevant entities. The protection of secrecy of the message depends on the confidentiality and secure distribution of the secret key. Figure 1 illustrates the schematic diagram of symmetric key encryption and decryption procedure. The selective encryption algorithms are used just to encrypt certain portions of the messages with less overhead consumption but simultaneously sufficient messages are encrypted to provide reliable safety to secure the confidentiality of the transmitted message.].

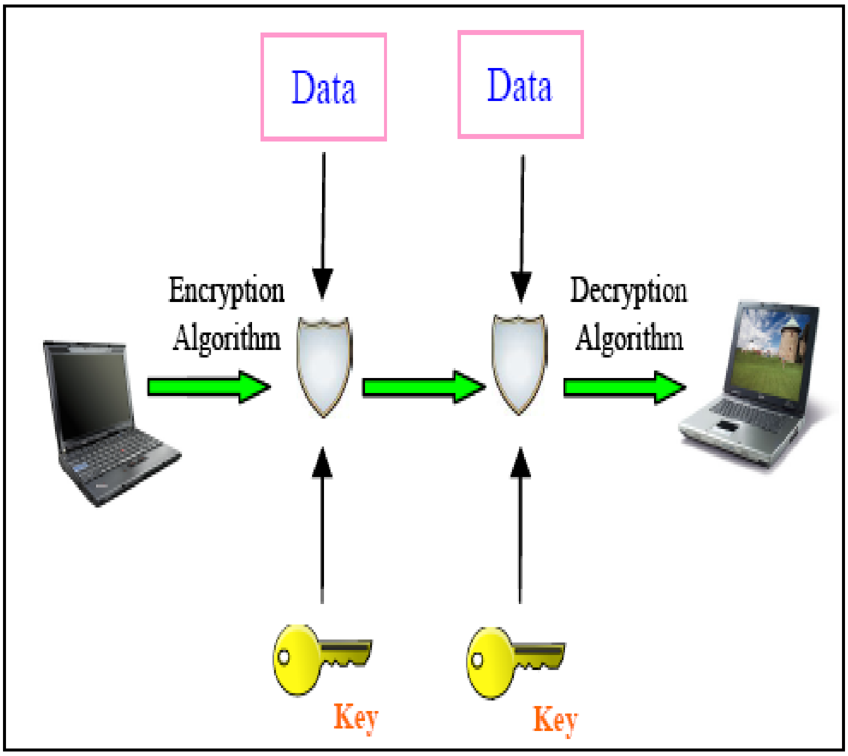

Figure 1: An example of encryption and decryption processes

There is no need to encrypt all messages in selective encryption algorithm while the entire data transmission can be viewed to be secure on the whole. Selective encryption algorithm improves the scalability of data transmission and reduces the processing time. The primary application of selective encryption algorithms is found in the realms of energy-aware environments or large scale data transmission like multimedia communications, mobile ad-hoc networks and wireless sensor networks etc [8]

II. LITERATURE REVIEW

Wireless communications have received a lot of attention from both industry and academic groups. Wireless access allows independency between the user's position and the physical bearer used to access services from the network, as well as, it supports the delivery of multimedia content ubiquitously(Chiti[1]) (Akyildiz & Wang [2]).

Nowadays, the Wireless Mesh Network (WMN) model is one of the most relevant approaches to provide last mile access in emerging communication systems (Held, Zhang [3]) (Hossain & Leung[4]), such as The Institute of Electrical and Electronic Engineers (IEEE) 802.11s (802.11s, 2010).

WMNs are a special case of ad hoc networks, which allow multiple hops, increase the coverage area, and have low implementation cost and support ubiquitous features for Internet access. Multimedia applications, such as video streaming, Voice over IP (VoIP), and Internet Protocol Television (IPTV), will be abundant in future wireless mesh systems and, consequently, the end-to-end quality level support for these services is a major requirement for a near future. Shivanajay Marwaha, Jadwiga Indulska, Marius Portmann[5] have analyzed different challenges and advances in the QOS provisioning in WMNs, stating the problems or challenges before the technology and biggest problem of power consumption while encryption and decryption

.

III. METHODOLOGY

[1] Selective Encryption :

The selective encryption algorithm is to just encrypt certain portions of the messages. They can reduce the overhead spent on data encryption/decryption and improve the efficiency of the network. The design of a selective encryption algorithm with less processing time but with relatively high security level is extremely significant. Figure 2 show the schematic diagram of a selective encryption process.

When the communicating data is scalable or a network is aware of its limited computational resources, it is not really needed to provide full security protection on all exchanged information. As a major selective encryption methodology, the probabilistic method [1] provides sufficient uncertainty to a selective-based cryptosystem. In order to adapt the scalability and to improve the processing capacity of a cryptosystem, the cryptosystem just partially encrypts the transmitted messages that it wants to protect based on a certain probability. The probabilistic method is involved in the procedure of selective encryption, so that those selected messages are encrypted in a deterministically random way. By means of the inclusion of probability, nobody will exactly know which messages are encrypted except the communicating parties. Thus, even if there are malicious attackers which are able to intercept the communicating messages, they still cannot fully obtain the selectively encrypted messages or reconstruct all messages

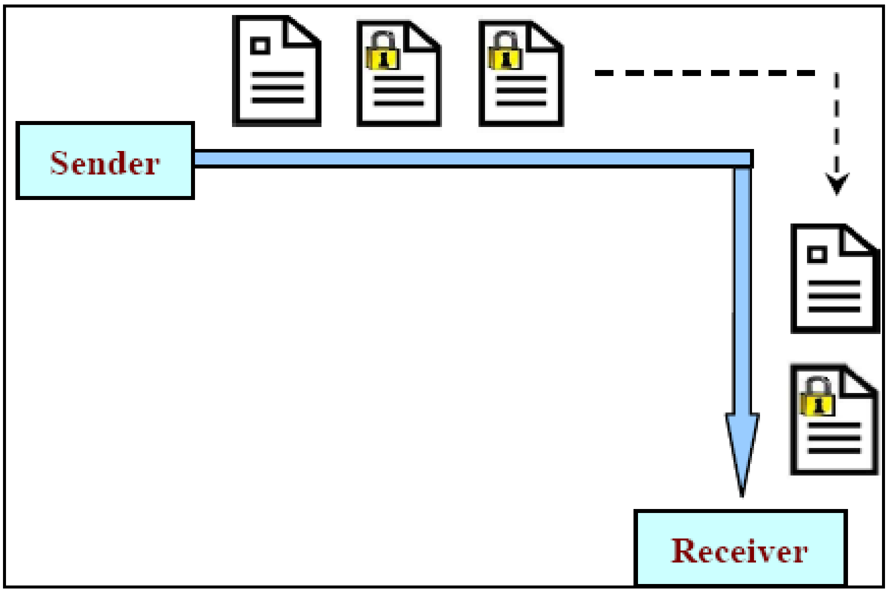

Figure 2: The schematic diagram of selective encryption

.

a) A Toss-A-Coin Selective Encryption Algorithm:

All transmitted messages are divided into two groups: the odd number messages and the even number messages. For instance, messages *M1, M3, M5, ... M(2n-1)* represent the odd number messages; messages *M2, M4, M6, ... M(2n)* represent the even number messages. When the sender needs to decide which group should be encrypted, it makes use of a toss-a-coin method to determine whether the even number messages or odd number messages are to be encrypted. Hence, the value of encryption ratio here is tentatively determined to be 0.5, which means that approximately 50% of the communicated data will be encrypted.

b) A Probabilistic Selective Encryption Algorithm:

A Probabilistically selective encryption algorithm uses the advantages of the probabilistic methodology aiming to obtain sufficient uncertainty. During the process of sending messages, the sender will randomly generate a value to indicate the encryption percentage, which represents how many messages will be encrypted among the transmitted messages. Then the sender uses a probabilistic function to choose the already deterministic amount of messages to encrypt them, in order to increase the uncertainty in the process of message selection. Figure 3 illustrates the flow chart of the probabilistic selective encryption algorithm.

[2] The probabilistic selective encryption algorithm is comprised of the following three steps:

a) The sender of communicating parties *S* will first apply a Random Number Generator (*RNG)* to randomly obtain an encryption ratio *er*, which determines the percentage of encrypted messages among all messages. Here, in order to ensure that enough data is able to be encrypted so as to provide sufficient security protection, the generated encryption ratio should be higher than a pre-determined value of security requirement *SR* (*SR* means that data communication is secure if there is *SR* or more percentage of messages are encrypted).

$$S \xrightarrow{RNG} er \mid \{er \geq SR\} \qquad (1)$$

b) Then the sender *S* will employ a probabilistic function *PF* to generate an encryption probability *pi* to determine if one message *Mi* will be encrypted or not.

$$S \xrightarrow{PF(M_i)} p_i \qquad (2)$$

$$p_i = \frac{\text{Counts Encrypted Messages}}{i}$$

c) The sender selects the messages to encrypt based on the above pre-determined encryption ratio *er*. For example, once *S* finds out that the encryption probability *pi* is less than or equal to the encryption ratio *er*, it will encrypt the message *Mi* using its secret key *SK,* otherwise this message will not be encrypted accordingly.

$$\begin{cases} S \rightarrow \mathrm{SK}[\mathrm{M}_i] & \mathrm{p}_i \leq er \\ & \qquad (3) \\ S \rightarrow \mathrm{M}_i & \mathrm{p}_i > er \end{cases}$$

d) Thus, the probabilistic selective encryption algorithm integrates both the probabilistic method and stochastic strategy in order to increase the uncertainty in the process of message selection.

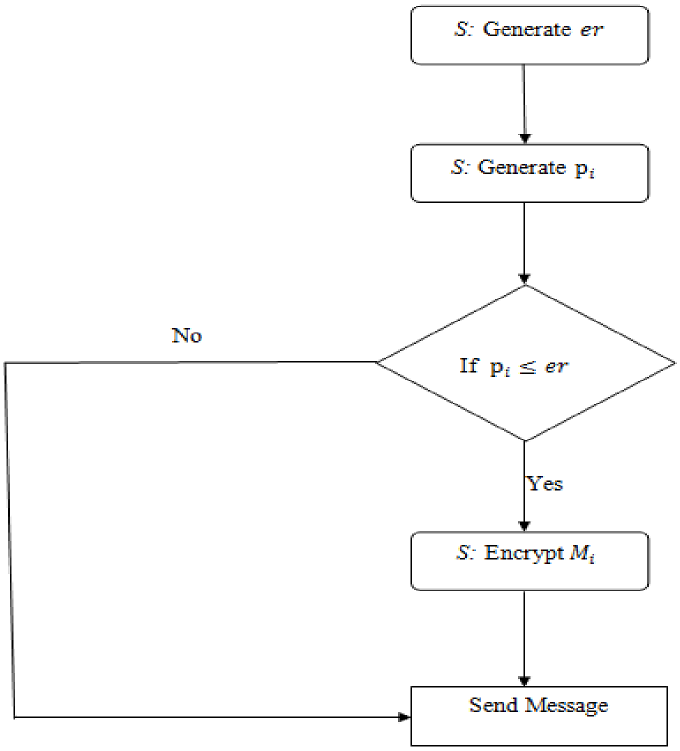

Figure 3: The flow chart of probabilistic selective encryption algorithm

[3] Proposed Method of Selective Encryption Algorithm:

Our proposed selective encryption algorithm is based on message entropy. Using the message entropy the uncertainty in the process of message selection is increased. Following is the proposed algorithm for selective encryption.

where,
$\mathrm{E}(m)$= Entropy of message
$\mathrm{Thr}(m)$= Threshold value of message
N0= Number of 0's bits
N1= Number of 1's bits
N= Total number of bits

Step 0: Take messages one by one

Step 1: Calculate $\mathrm{E}(m)$ = Entropy of message

1.1: Convert message to ASCII code.
1.2: Convert the ASCII code to binary format.
1.3: Find the number of 0's say N0 and the number of 1's say N1
1.4: Calculate N0=N0/N, N1=N1/N.
1.5: The entropy of the message will be,

$\mathrm{E}(m)$= - (N0*$\log_2(N0)$ + N1*$\log_2(N1)$)

Step 2: This is the first message then,

$$\mathrm{Thr}(m) = \mathrm{E}(m)$$

If previously encryption percentage is less than equal to 50% then,

$\mathrm{Thr}(m) = \mathrm{Thr}(m) - \mathrm{E}(m)*1/100$

Else If previously encryption percentage is more than 50% then,

$\mathrm{Thr}(m) = \mathrm{Thr}(m) + \mathrm{E}(m)*1/100$.

Step 3: If $\mathrm{E}(m) >= \mathrm{Thr}(m)$ then Encrypt the message
else do not encrypt the message.

Step 4: Calculate encryption percentage.
Step 5: Take the next message till all messages to be sent are over.

In selective encryption, if messages that have all 1s or 0s are encrypted without encrypting messages that have higher entropy in that case the security reduces. The proposed method selectively encrypt the messages having higher entropy based on encryption percentage and passes the messages which have lower entropy without encryption. Passing the messages having lower entropy without encryption increases security of transmission and reduce the power for wireless ad-hoc networks. The proposed method provide more security and saving time as compared to the probabilistic method. Figure 4 illustrates the flow chart of the proposed selective encryption algorithm.

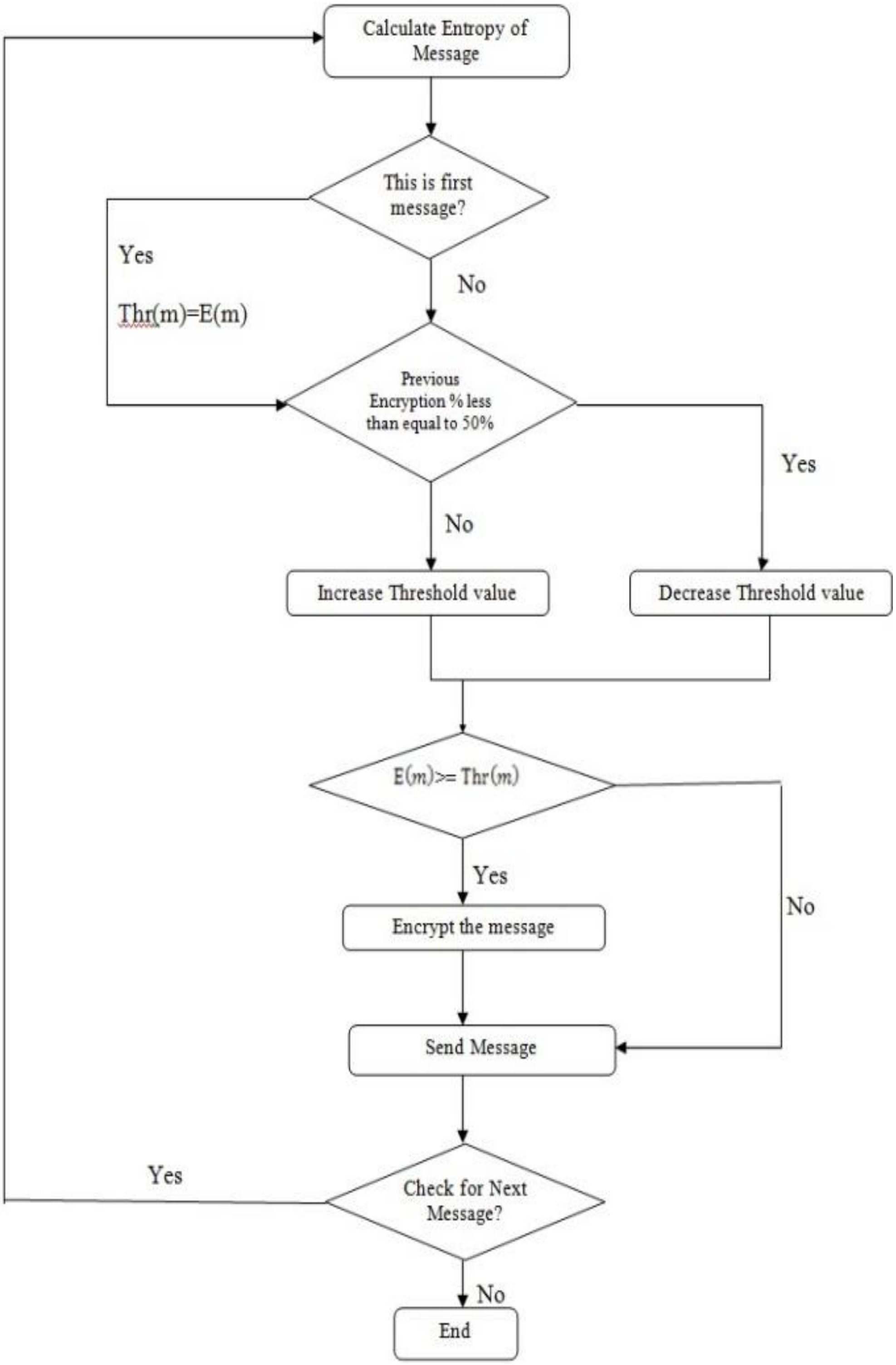

Figure 4: The flow chart of proposed selective encryption algorithm

IV. Results and Conclusions

The proposed algorithm selectively encrypt the packets having higher entropy based on encryption percentage and passes the packets which have lower entropy without encryption. The higher entropy contain more data as compared to the lower entropy. The probabilistic algorithm encrypt the packets based on encryption ratio and not on the amount of data inside the packet. As compared to the probabilistic algorithm the proposed selective encryption algorithm provide more uncertainty in the process of packet selection, hence provides greater security.

E.G -1: 40 packets

Probabilistic Algorithm	Proposed Algorithm

message_count = 14
encrypted_message_count = 8
pi = 0.5714285714285714
er = 0.57926858629997291
Node(0) Sending -> data at 48.0
- contents: ge
- encrypted: uÃ–Je
	message_count = 14
	encrypted_message_count = 6
	E_M_bits = 0.811278124459132 83
	E_Thr = 1.0112951854171077
	pi = 0.42857142857142855
	er = 0.5
	Node(0) Sending -> data at 39.0
	- contents: ge
	- encrypted: ge

message_count = 28
encrypted_message_count = 16
pi = 0.5714285714285714
er = 0.57926858629997291
Node(0) Sending -> data at 93.0
- contents:
- encrypted: pÃ“Â‰b'ÂŠ
	message_count = 28
	encrypted_message_count = 15
	E_M_bits = 0.5435644431995964
	E_Thr = 0.91850327934280085
	pi = 0.5357142857142857
	er = 0.5
	Node(0) Sending -> data at 87.0
	- contents:
	- encrypted:

E.G-2: 60-packets

PROBABILISTIC ALGORITHM	PROPOSED ALGORITHM

MESSAGE_COUNT = 32
ENCRYPTED_MESSAGE_COUNT = 18
PI = 0.5625
ER = 0.57168566778846353
NODE(0) SENDING -> DATA AT 105.0
- CONTENTS: IN O
- ENCRYPTED: CL@Ã¡Â¯CÂ€
	MESSAGE_COUNT = 32
	ENCRYPTED_MESSAGE_COUNT = 14
	E_M_BITS = 0.87743731108963297
	E_THR = 0.98886920345776241
	PI = 0.4375
	ER = 0.5
	NODE(0) SENDING -> DATA AT 90.0
	- CONTENTS: IN O
	- ENCRYPTED: IN O

MESSAGE_COUNT = 41
ENCRYPTED_MESSAGE_COUNT = 23
PI = 0.56097560975609762
ER = 0.57168566778846353
NODE(0) SENDING -> DATA AT 133.5
- CONTENTS: SEL
- ENCRYPTED: Âº_Ã‹Â±Â¬ÃµV<
	MESSAGE_COUNT = 41
	ENCRYPTED_MESSAGE_COUNT = 22
	E_M_BITS = 0.85714843742837177
	E_THR = 0.95743743015141014
	PI = 0.53658536585365857
	ER = 0.5
	NODE(0) SENDING -> DATA AT 127.5
	- CONTENTS: SEL
	- ENCRYPTED: SEL

The above examples show that, probabilistic algorithm encrypts packets having less information. Hence, we conclude that the proposed algorithm saves encryption time and provides more security than the probabilistic algorithm.

Table shows the comparison of selective encryption algorithms.

Characteristics	Encryption Time Percentage	Encryption Time	Saving Time	Security
Algorithms				
1) Toss-A-Coin	Approximate 50%	Less	More than other two methods	Less Secure
2) Probabilistic	50% or More than 50%	More	Less than other two methods	Secure
3) Proposed	50% or More than 50%	Medium	More than probabilistic method	More Secure

Wireless mesh network is a rapid deployed, self organized technology. Provisioning of QoS in rural WMNs is the challenging task. Selective encryption algorithms is one of the most promising solutions to reduce the cost of data protection, reduce the computation time and power in wireless and mobile networks. They can reduce the overhead spent on data encryption/decryption and improve the efficiency of the network. The proposed selective encryption algorithm in comparison with the probabilistic algorithm gives better results in terms of time and security. Selective encryption involves more uncertainty to data encryption, hence provides greater security. The results demonstrate the effectiveness of using a proposed algorithm to achieve selective encryption in wireless networks and the approach has a better performance when compared to other approaches. Thereby, the proposed selective encryption approach provides a feasible solution for secure wireless communication and provides more battery backup to the nodes by reducing the security overheads.

ANOWLEDGMENTACK

We would like to acknowledge the Students of Computer Science & Engineering Department, SVERI's College of Engineering, Pandharpur for their support. I Mr. Amrut Pawar specially want to thank my guide Prof. Amit R. Sarkar for their guidance.

REFERENCES

[1] Chiti, F.; Fantacci, R.; Maccari, L.; Marabissi, D. & Tarchi, D. A broadband wireless communications system for emergency management, Wireless Communications IEEE, Vol.15, No.3, (June 2008) page numbers (8-14)

[1] Akyildiz, I. & Wang, X. (2009). Wireless Mesh Networks (Advanced Texts in Communications and Networking), Wiley Held, G. (2005). Wireless Mesh Networks, Auerbach Publications

[2] Hossain, E. & Leung, K. (2009). Wireless Mesh Networks: Architectures and Protocols, Springer US

[3] Challenges and Recent Advances in QoS Provisioning in Wireless Mesh Networks Shivanajay Marwaha Jadwiga Indulska Marius Portmann 978-1-4244-2358-3/08/$20.00 © 2008 IEEE

[4] Yonglin Ren, Azzedine Boukerche ,Lynda Mokdad, "Performance Analysis of a Selective Encryption Algorithm for Wireless Ad hoc Networks", IEEE WCNC 2011-Network.

[5] K.VetriVel, Dr.C.Senthamarai, "A Study of Comparison of various Block Ciphers in Symmetric Key Encryption Algorithm", International Journal of Computer Information Systems, Vol.1, No.5, 2010.

[6] S.Kala, "Enhanced Selective Encryption Algorithm For Wireless Ad Hoc Networks", International Journal of Computing Technology and Information Security Vol.1, No.2, pp.48-51, December-2011.

[7] Priyanka Agrawal, Manisha Rajpoot, "Partial Encryption algorithm for Secure Transmission of Multimedia Messages", International Journal of Computer Science and Technology(IJCST), Vol.3, Issue 1, Jan-March 2012.

[8] M. Abomhara, Omar Zakaria, Othman O. Khalifa, A.A Zaidan, B.B Zaidan, "Enhancing Selective Encryption for H.264/AVC Using Advanced Encryption Standard", International Journal of Computer Theory and Engineering, Vol.2, No.2 April, 2010. "PDCA12-70 data sheet," Opto Speed SA, Mezzovico, Switzerland.

[9] Bismita Gadanayak, Chittaranjan Pradhan, "Selective Encryption of MP3 Compression", International Conference on Information Systems and Technology (ICIST) 2011, Proceedings published by International Journal of Computer Applications® (IJCA)2011.