Journal of Theoretical and Applied Information Technology
20th October 2014. Vol. 68 No.2
© 2005 - 2014 JATIT & LLS. All rights reserved·

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

NMULET: IMPROVING THE QOS IN TERMS OF SECURITY FOR WIRELESS SENSOR NETWORKS

[1]M.RAJENDIRAN, [2]Dr.C.NELSON KENNEDY BABU.
[1] Research Scholar,Anna University,Chennai. India.
[2] Principal,CMS Engineering college,Namakkal,Tamilnadu ,India.
E-mail: [1] mrajendiran@gmail.com, [2] cnkbabu63@gmail.com

ABSTRACT

WSNs are infrastructureless framework and pass on by method for remote medium. Furthermore on account of the eminent attributes and characteristics of WSN they are used as a piece of climbing procurements like surveillance checking, center and military, remote zone. Generally sensor nodes are having adaptability lead the correspondence around the nodes happen by method for multi-bounce without any stipulations. It makes some piece of possible conclusions for distinctive feeble ambushes in WSN. In the current framework MULET computation was proposed for encoding and translating plain substance by mapping the characters clearly to the Unicode and it could be recognized by the aggressors successfully. The main objective of this paper is to provide a high security to improve the quality of service of WSN in terms of security. In this paper NMULET-[Novel Multi Language Encryption Technique] approach based estimation is exhibited for secure key time for encoding and unscrambling the data transmitted around center points. NMULET helps SOUTH-INDIAN languages based Key period and for more efficacies a gathering of Cryptographic strategies [md5, SHA-1, and CSHA-1] are given to customer choice. The examination conclusions show that NMULET gives more secured data transmission in WSN. Quality of Service in terms of Security is improved without affecting the network characteristics using NMULET is proved in this paper.

Keywords: *Wireless Adhoc Networks; Energy Efficiency; Novel Clustering Approach; Clustering.*

1. NOMENCLATURE

Symbols	Description
MANET	Mobile Adhoc Network
MULET	Multi-Language Encryption Technique
AES	Advanced Encryption Standard
DES	Data Encryption Standard
NMULET	Novel MULET
ECC	Elliptical Curve Cryptography

2. INTRODUCTION

The electronic age has pushed a substantial consolidation of hardware and correspondence in human life. It, on one hand, wonderfully streamlined the human life and on other hand it has additionally put a considerable measure of security difficulties for our interchanges and transaction. Security of correspondence frameworks intensely relies on upon the security of cryptographic results joined. Various eves-droppers, programmers, cryptanalyst, in this manner, eye on these results just. Their steady deliberations over a time of time have offered ascent to disclosure of various cryptanalytic strike. For system based frameworks encryption methods two sorts of systems viz., deviated key encryption including RSA and ECC [4] and symmetric key encryption including AES, DES [2] and IDEA and so on. An alternate class that has advanced itself from traditional encryption procedures is the multi dialect encryption system. A not many systems have been proposed as of late. One of such method named MULET has been proposed in [1].we have examined the encryption strategy in subtle elements and watched shortcoming in the calculation. In this paper we introduce our perceptions and adjustment of the system. We can additionally dissection the playing point of the new plan over the MULET plan [3]. In the accompanying area 2 we display N-MULET calculation in a word and in segment three and examine inadequacies and the changes. In area 4, we exhibit our calculation and test vectors. In the conclusion segment we examine the benefits of the adjusted strategy and the conceivable growth of the work. As examined over, the Multilanguage encryption is the region where just a couple of plans have been proposed. Separated from MULET, there is an alternate plan named N-MULET. It is a key based Multilanguage encryption plan [1].

3. RELATED WORKS

A not many systems have been proposed work as of late. One of such strategy named MULET has been proposed in [3].we have examined the encryption procedure in subtle elements and watched shortcoming in the calculation. In this paper we exhibit our perceptions and our adjustment of the strategy. It is likewise examination the point of interest of new plan over the MULET plan. It was proposed a calculation in Multilanguage approach, which produces diverse figure writings at distinctive time for the same plaintext over a scope of dialects backed by Unicode. It has a superior recurrence dispersion of characters in the figure content than past deal with this methodology [8].

As talked about over, the Multilanguage encryption is the zone where just a couple of plans have been proposed. Separated from MULET, there is an alternate plan named MANET proposed by Prasenjit Chaudhary et. al. It is a key based Multilanguage encryption scheme[5]. Security issues of MANET are examined in [6]. Strikes misusing these issues are proposed in [7]. Quantum cryptography was introduced for heavy security in WSN [9].

4. EXISTING SYSTEM

In remote sensor arrange, the strength is not ensured since it is dynamic. Because of enhance the security and related elements including system life time, the energy usage is minimized by sparing the node energy by arranging the steering convention based the clustering instrument. In this paper a Novel Cluster based energy proficient steering convention is proposed for sparing the energy at the most extreme contrasting and the current protocols and the complete usefulness is given in the following segment.

5. PROPOSED APPROACH

There are different strike influences the information in WSN throughout transmission. A portion of the strike interfering with information is Sinkhole, Sybil and Wormhole and so on. Sinkhole is a noxious node which is accessible on the course where it never passes the gained information from the past node. It holds all the accepted information bundles without anyone else's input. Whereas Sybil is an alternate sort of noxious node when it comes closest to different nodes in the course, it interrupts the physical data about the node and act like that node. Recognizing this sort of ambushes, despite the fact that the assailant interrupts the information parcel, the information is not accessible to the assaulter in understanding [readable] design since the information holds ID, Language –ID, NMULET based UDC and scrambled utilizing a particular encryption calculation.

NMULET gives more security to information transmission around nodes in WSN. NMULET calculation is installing a Unicode into plain content and believers into garbled content alongside the key created from the Unicode and it is exceptionally discernible that with the exception of that specific Unicode key unscrambling is inconceivable. In the blink of an eye the late mystery correspondence happens in huge way in makeshift developing system as WSN. The general usefulness of the paper is demonstrated below

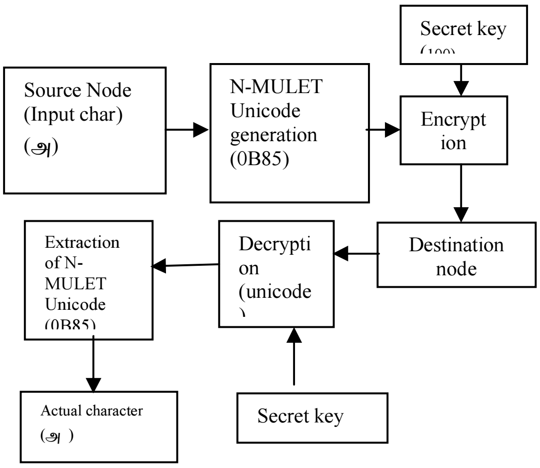
Secret key (100)
Source Node (Input char) (அ)
N-MULET Unicode generation (0B85)
Encrypt ion
Destination node
Decrypti on (unicode)
Extraction of N-MULET Unicode (0B85)
Actual character (அ)
Secret key

Figure-1:Proposed Model

6. NETWORK MODEL

Since this paper concentrate on mystery correspondence in WSN utilizing NMULET system let a system is built utilizing N number of nodes. In WSN G, N number of nodes is conveyed haphazardly. A base station BS is accepted and every node capacities under the screen of BS. At the time of correspondence around the nodes the mystery and the cryptography might be connected to acquire the security in WSN.

7. NMULET

NMULET calculation can insert an Unicode with the plain content and proselyte into garbled content alongside the mystery key. The Unicode is all inclusive character which is free to an extent of dialects on the planet. The NMULET calculation fundamentally holds of three capacities viz. key era, Encryption ( ) and unscrambling ( ).

While passing the message the message could be install into Unicode where the Unicode might be made as per the dialect and the dialect characters. Utilizing the recently created Unicode key the information could be scrambled and transmitted. The same way the information might be unscrambled in the other beneficiary end and it is portrayed in Figure-2.

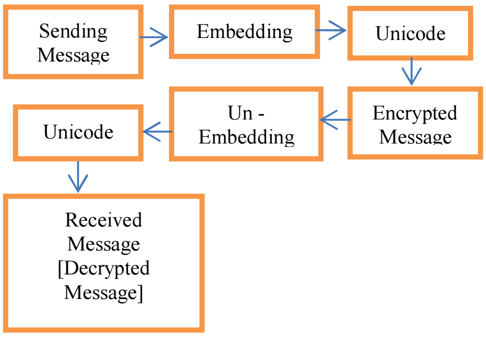

Figure-2: NMULET

The main encryption, decryption mechanism is common for certain languages which can understand by the computer. For various SOUTH-INDIAN languages character set range is given in Table-1 [10].

Language	Range
Tamil	0B80 – 0BFF
Kannada	0C80 – 0CFF
Telugu	0C00 – 0C7F
Malayalam	0D00 – 0D7F

Table – 1: The Unicode Character Range for a Range of Languages.

Keeping in mind the end goal to define the extent of the character mapping to the Unicode for the south Indian dialects and the reach for 0b80 – 0bff [10] detail Tamil dialect, 0c80 -0cff is the Unicode extent details Kannada Language, 0c00 – 0c7f is the Unicode range for Telugu dialect and 0d00 – 0d7f indicates Malayalam Language. For mapping the Unicode for the dialects characters, the initial two characters shows the dialect ID and the following two characters demonstrates character ID. The Language ID getting changed as per the dialect and the Character ID getting changed as indicated by the characters taken in that specific dialect and it is demonstrated in Figure-3.

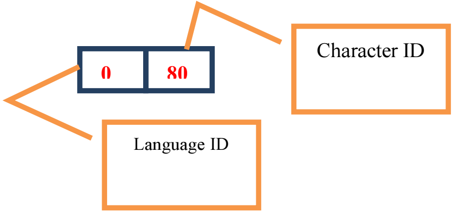

Figure-3: Language ID mapping with Character ID

NMULET uses a 3-bit code to represent one character which includes ‘0’, ‘1’, and ‘2’. It starts from ‘000’ and totally 27 combinations. Because of the Unicode is in hexa-decimal format, the some of the UDC code is represented for mapping the standard characters from ‘0’ to ‘F’ is given in Table-2. In the entire 27 combinations 16 are utilized for hexadecimal combinations (‘0’ to ‘F’). The other 10 are reserved for special characters mapping and it is common in any language.

Hex Character	User Defined Character
0	001
1	010
2	011
3	100
4	101
5	110
6	122
7	002
8	020
9	022
A	200

B	202
C	220
D	211
E	112
F	121

Table – 2: User Defined Codes Using 3 Bits.

The UDC code can be assigned to the corresponding Unicode value mapping the language characters and it is clearly depicted in the following Table-3. Example the character 'அ' is assigned by 0B85, where the user defined code is 001202112112.

Character	Unicode Value	User Defined Code
அ	0B85	001202020110
K	0BAE	001202200112
◌்	0BCD	001202220211
k	0BAE	001202200112
H	0BBE	001202202112

Table – 3: Language Characters With UDC

The dialect based characters and its equal characters are allocated in the accompanying table-4. There are four dialect is taken for testing the proposed methodology. All the dialect has its number of character set and its Unicode values. Utilizing the above blending mapping the characters from any dialect is taken to make Unicode and all inclusive code for correspondence. The specific dialect code is changed over into Unicode.

The created UDC is taken as the key for scrambling the information and the measure of the key could be dependent upon 256. However in this paper the key size is confined as 32 to 64. The size of the key may surpass till 256 is not right.

At that point as indicated by the Novel MULET system, the encoded information is scrambled and sends to the objective from the source node. The whole encryption and Decryption technique in this paper is given underneath.

(*a*) Encryption Module: The Encryption Module has more options like MD5, SHA-1, CSHA-1 etc., where the user can select any one which they considered as best. The input message embedded Unicode is encrypted by the selected algorithm.

(*b*) Decryption Module: The Decryption Module has the same options where the user should select the algorithm through which the encryption was obtained. The decrypted result is purely depends on the corresponding algorithm selection.

The complete usefulness of NMULET is connected in a course while information transmission of WSN. At the point when a node S begin making an impression on its next bounce a portion of the crucial data about the node is additionally passed along the information. After a course coveted for information transmission, the node ID, dialect, MSG – [message] is taken from the information bundle for get ready NMULET code. Utilizing the code, the information is scrambled [where the client ought to pick the encryption algorithm] and went to the following bounce is demonstrated in Figure-4.

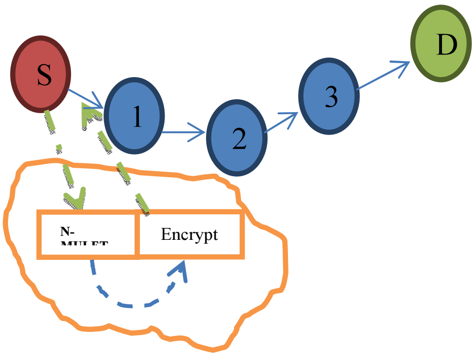

Figure-4: Secured Data Transmission

The usefulness of NMULET based secured information correspondence in a WSN is composed in a manifestation of Algorithm for executing and confirming the viability of the proposed methodology. The information parcel transmitted from source node to objective node are encoded and scrambled at source and unscrambled and decoded in the end of the line. The accompanying calculation represents the usefulness of the N-MULET.

```
$Algorithm\ N - MULET\ ( )$
{
    $Let\ G\ be\ a\ WSN,\ \ G = \{ N_1, N_2, \ldots\ldots, N_N\}$
    $Ni\ is\ a\ self\ analysing\ sensor\ node$
    $Let\ N_s\ be\ the\ source\ node, and\ N_D\ be$
        $the\ Destination\ node$
    For I = 1 to N
        ID(Ni) = Node_Number;
        MSG(Ni) = Node_Message;
        L = Language;
    End for
    $For\ I\ = 1\ to\ M$
        $Key(Ni)\ -> NMULET\ (MSG\ (Ni), L)$   // encoding
        $Data\ (Ni) = Encry(Data(Ni), Key(Ni))$   // encryption
        $Data\ (Ni + 1) <- Data\ (Ni)$   // passing to next node
    $End\ for$
    $Data\ (Nm) = NMULET\ (Decry(Data\ (Nm - 1), Key\ (Nm - 1)))$
// at Destination node decrypt and dcode
}
```

When the node transmits the data it will be encoded and decoded according to the language. The encoding and decoding depends on the language and Unicode character, user defined characters. For encryption, decryptions there are three methods [MDS, SHA-1, and CSHA-1] are given to the user, where the user can select any one of a language according to their need. The encryption and decryption methods are given in the format of algorithm and it is shown below.

```
$Algorithm\ Encry\ (\ D, K)$
{
    $Option\ = \{MDS, SHA - 1, CSHA - 1\}$;
    $Switch\ Option$
    {
    Case 'MDS':
    {
    $Return\ MD5\ (data\ (Ni), Key\ (Ni), hash)$;
    }
    Case 'SHA':
    {
    $Return\ SHA\ (data\ (Ni), Key\ (Ni), hash)$;
    }
    Case 'CSHA − 1':
    {
    $Return\ CSHA\ (data\ (Ni), Key\ (Ni), hash)$;
    }
    return data
    }
}
```

7.1 Numerical Illustration Of NMULET

For example Node-0 transmits a HELLO packet to Node-2 means; the NMULET can create the key for Node-0 is

Node-1	Tamil	HELLO

Table-4: Packet Format from Node-1

Where the node-ID is 1, the Language is Tamil and the Message is “HELLO”. NMULET process on this Table-4 content can be written as:

10B8 is the character where the UDC is

10B8 010001202020

The key obtained from NMULET is “010001202020” and the encryption method taken for encryption is SHA-1 means the encrypted data is:

FI79JS93JHDKD83HDKDNJDHXZNXKD8765 is the encrypted data.

The source node transmits the encrypted data to the next hop. The next hop simply passes it to its next neighbor hop. This cyclic process can be repeated until the find the destination node D. once the destination node receive the encrypted data, it decrypt the data using the key received earlier from the source node.

8. SIMULATION SETTINGS

In order to implement and evaluate the security for WSN using NMULET approach, the Network Simulator-2 software is suggested and the parameters are assigned for setting the simulator is depicted in the following Table-5.

Simulation Parameter	Value
Area	1000m x 1000m
Speed	1 to 15 m/s
Radio Propagation Model	Two-ray ground reflection
Radio Range	250 m
Number of Nodes	20 to 1000
MAC	802.11
Application	CBR, 100 to 500
Packet size	50
Simulation Time	100 s
Placement	Random
Malicious Population	Up to 5%

Table-5: Simulation Settings

To demonstrate that the NMULET system is more compelling and productive than the current strategy, the NMULET calculation is reproduced in Ns2. The system zone size is 1000 x 1000 and the amount of nodes taken for recreation is 20, and the front end of the reenactment is composed in TCL and backend coding is composed in .cc code. Figure-3 shows the system sent with 20 amounts of nodes and how the nodes are named and how they correspond with one another. Throughout the correspondence NMULET connected and it is indicating that, how the source node passing the information to the objective node safely.

Encryption of different messages from distinctive dialects might be effectively completed with the assistance of MULET calculation. This is most likely the trademark characteristic of the calculation as it makes ready for the confinement of programming in cryptographic space. It is additionally an intriguing certainty that substitution technique might be effortlessly connected when we have progressive reiteration of characters. This component is likewise exceptionally viable secluded from everything the amount of characters in the figure content and therefore makes it to a great degree troublesome for the interlopers to anticipate two message sizes.

9. RESULTS AND DISCUSSION

NMULET calculation is actualized in TCL and the outcomes are given beneath. All the three encryption, unscrambling instrument is noncompulsory for the client, where the client can select any one the technique around the three. The accompanying Table-6a, Table-6b and Table-c shows the data, yield of the encryption, decoding components given in this paper.

```
Input String:  Good Morning

MD5-Encryption-output    :
72a079088694099d64753fdba3bfe26e

MD5-Decryption-output    : Good Morning
```

Table-6a: Input-Output For MD5 Algorithm

```
Input String         : Good Morning

SHA-1 Encryption output  :
06e336231466d0b0573a05cbca7813444afb5b29

SHA-1 Decryption output  : Good Morning
```

Table-6b: Input-Output For SHA Algorithm

```
Input String: Good Morning

CSHA-1 Encryption output             :
8BCEFA4C1EDE0AE9CC24B32AB292BB25D07
1ED42

CSHA-1 Decryption output : Good Morning
```

Table-6c: Input-Output For CSHA-1 Algorithm

The trouble making of the vindictive nodes in the system is fused as the same as done in [10]. By executing the proposed approach in TCL with different amounts of nodes conveyed in the system like 10, 20, 30, 40 and 50 nodes. The rowdiness node is identified just by confirming the key and the encryption-decoding procedure. It implies if and if the node has a place with the specific system and in the specific course, it is considered correspondence. As per the nodes and reproduction adjust the outcome is created and given in diagram structure for examining the execution.

While recreation the paramount elements of the system like energy, noxious node recognition rate and the throughput are caught from the follow document produced naturally and plot as a diagram. The accompanying Figure-5 shows the amount of vindictive nodes caught in various adjusts in a stipulated time of time by the proposed approach and the current methodology.

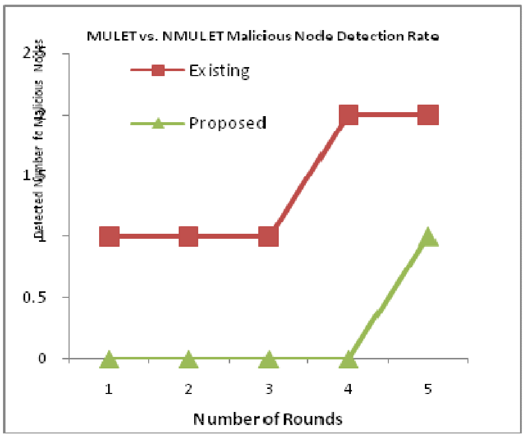

Figure-5: MULET Vs. NMULET Comparison In Terms Of Malicious Detection Rate

The amount of pernicious node caught by the proposed methodology is short of what the current methodology since the malevolent action is lessened in the proposed approach in the introduction of the system itself. Despite the fact that a few less number of nodes attempted from outside the system to go about as noxious and it is caught correctly by the proposed methodology and the discovery rate is indicated in the Figure-5 plainly.

Agreeing the sinkhole assault the NMULET methodology is contrasted and the LBIDS [11] approach and the discovery rate is given in the accompanying Figure-6, where the NMULET controls the action of sinkhole ambush than the LBIDS approach.

In each one adjust the amount of aggressor recognized in LBIDS for 10 nodes is 1, 20 nodes is 2, 30 nodes is 3, 40 nodes is 4 and for 50 nodes is 5. Where in NMULET there is no assaulter caught up to 40 amounts of nodes demonstrated in Figure-6. While sending 50 number of nodes the amount of aggressor identified is 1. Consequently the NMULET is controlling the sinkhole ambush than different methodologies talked about prior.

It is expected that in the event of any possible strike may get the information in the course; the ambusher can't get the information to the extent that effortlessly from the scrambled information group due to the NMULET based key era.

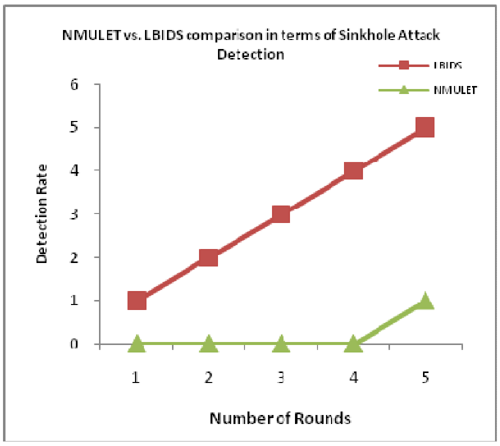

Figure-6: NMULET Vs. LBIDS

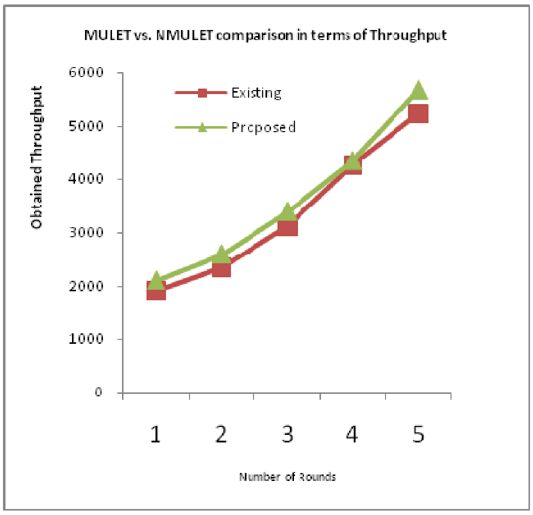

Figure-7: MULET Vs. NMULET Comparison In Terms Of Throughput

As far as throughput the proposed methodology got more fruitful transmission than the current methodology and it unmistakably delineated in Figure-7. The proposed methodology transmitted 2100, 2600, 3400, 4356 and 5688 parcels in all the four rounds with 10, 20, 30, 40 and 50 nodes separately where the current framework transmitted 1899, 2345, 3125, 4267 and 5234 bundles in all the four rounds with 10, 20, 30, 40 and 100 nodes individually.

9.1 Performance Matrices

To evaluate the performance of the NMULET approach the throughput, Packet delivery ratio, delay, routing overhead and energy are verified and shown in the following figures. And it is evaluated by changing the number of nodes as 10, 20, and 30, 40 and 50.

Throughput: The total number of data packets transmitted and received successfully within a stipulated time period.

Packet Delivery Ratio: The percentage of received data packets in the destination.

Energy: Remaining Energy of each node is summed after detecting the consumed energy.

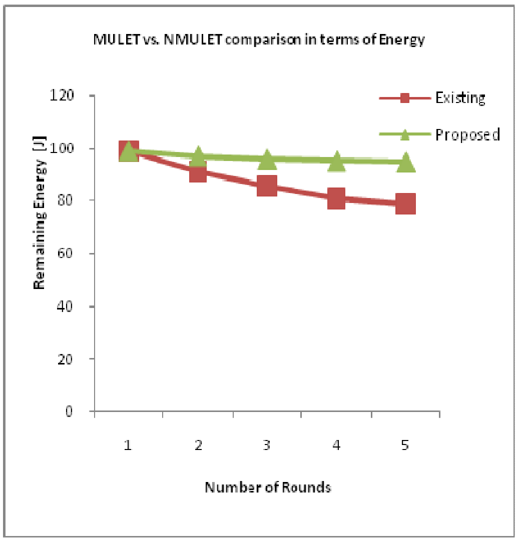

Figure-8: MULET Vs. NMULET Comparison In Terms Of Energy

If there should arise an occurrence of energy sparing the proposed methodology holds more energy than the current methodology and it plainly portrayed in Figure-8. The proposed methodology holds 99.12%, 97.19%, 96.02%, 95.23% and 94.86% of the energy in all the four rounds with 10, 20, 30, 40 and 50 nodes separately where the current framework holds 98.94%, 91.07%, 85.65%, 80.95% and 78.92% of the energy in all the four rounds with 10, 20, 30, 40 and 50 nodes individually.

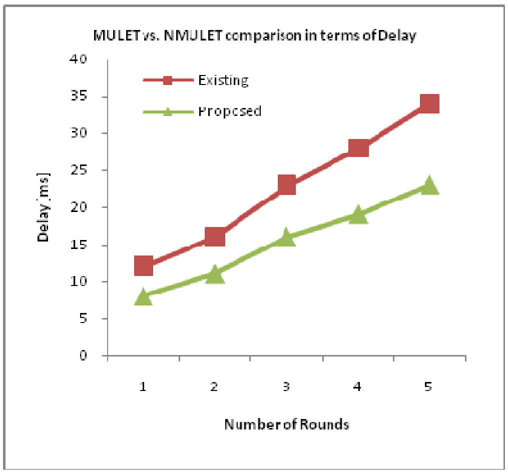

Figure-9: MULET Vs. NMULET Comparison In Terms Of Delay

In the event of postponement time taken by the proposed methodology is short of what the current methodology and it obviously portrayed in Figure-9. The proposed methodology takes 8, 11, 16, 19 and 23 seconds for all the four rounds with 10, 20, 30, 40 and 50 nodes individually where the current framework takes 12, 16, 23, 28 and 34 seconds for all the four rounds with 10, 20, 30, 40 and 50 nodes separately.

10. CONCLUSION

WSN basically need security and cryptographic methodologies to provide communication level and data level security during data transmission among nodes. There are various techniques introduced earlier to handle separately authentication and data encryption-decryption where it takes much time and cost and high complexity in process. Time, cost based security can be deployed simultaneously without any complexity NMULET was introduced and simulated in this paper. The specialty of NMULET approach is the Unicode based key generation where it can be used anywhere at any time in WSN.

NMULET calculation demonstrated above is checked through Ns2 reproduction and it says that the security in WSN might be gotten in preferable path over the current frameworks. The multi-choice cryptographic technique can fulfill the versatile nodes as far as security. The capacity of the NMULET calculation is working over distinctive SOUTH-INDIAN dialect spaces where it enhances the area measure in the system for limitless correspondence with high security. Additionally it is demonstrated that the QOS measurements in WSN is enhanced utilizing NMULET than the other leaving frameworks. Over all we might say that as till now this execution has been running effectively.

11. FUTURE WORK

NMULET can be improved and modified for any Language based secured data transmission and communication in WSN. This work is extended to global languages to enhance the security and QOS parameters.

REFERENCES:

[1] Kuldeep Bhardwaj, “Implementation of MULET (Multilanguage Encryption Technique) Algorithm “,International Journal of Theoretical and Applied Sciences 4(2): 25-32(2012).

[2] William C. Barker, "Recommendation for the Triple DataEncryption Algorithm (TDEA) Block Cipher", NationalInstitute of Standards and Technology, NIST SpecialPublication 800-67, (2008).

[3] G. Praveen Kumar, Arjun Kumar Murmu, Biswas Parajuli, Prasenjit Choudhury, "MULET: A Multilanguage Encryption Technique," itng, Seventh International Conference on Information Technology, pp.779-782, (2010).

[4] Elliptic Curve Cryptography, Certicom Research, 2000.

[5] Prasenjit Chaudhary et. al.”A New Multi-language Encryption Technique for MANET”,

[6] Nishu Garg, R.P.Mahapatra. “MANET Security Issues”. IJCSNS International Journal of Computer Science and Network Security, Volume.9, No.8, 2009.

[7] K. Rai et.al.”Different Types of Attacks on Integrated MANET-Internet Communication”, IEEE -2010.

[8] Anoop Kumar Srivastava, Sanjeev Sharma, Santosh Sahu, “MSMET: A MODIFIED & SECURE MULTILANGUAGE ENCRYPTION TECHNIQUE”, IJCSE – 2012.

[9] R.Sakthi Vignesh, S.Sudharssun, K.J.Jegadish Kumar, “Limitations of Quantum & The Versatility of Classical Cryptography: A Comparative Study, 2009 IEEE.

[10] The Unicode Standard, http://www.unicode.org, last visited: 14 May 2010.