International Journal For Technological Research In Engineering
Volume 5, Issue 12, August-2018 *ISSN (Online): 2347 - 4718*

A SECURE APPROACH OF DATA TRANSMISSION IN WSN USING RC5 ALGORITHM

Krishan Gopal[1], Yogesh Tiwari[2]
[1]M.Tech Scholar, [2]Assistant Professor HOD (ECE), Digital Communication, CGI Bharatpur Rajasthan.

Abstract: ***Wireless sensor network is the gathering of thousands of small sensor nodes, which have the capacity of detecting, processing and transmitting data in the network. The wireless sensor networks are constantly sent in threatening and inescapable condition. Security is significant worry in wireless sensor network. The customary network security techniques are not reasonable for wireless network on account of restricted asset, power and memory space. To address this issue, a lightweight key understanding convention is utilized. These protocols use the pseudo random number and bit astute activities, which are effective and plausible to sensor hardware. The topology of the wireless sensor network may change quickly and out of the blue. A standout amongst the most issues experienced in these networks, is security. In this exploration, lightweight convention utilizing dynamic key are proposed for taking care of the security issue. In this we utilize the Linear Congruential Generator to create the dynamic key. Dynamic key is like one time cushion. Dynamic key which is changed inevitably, every combine of encryption and decoding new key is created. The created lightweight convention utilizing diverse sorts of random number generator RC5 random number generator. The lightweight convention is contrasted with existing convention with locate the best technique for security. In this paper dynamic key is produced by utilizing distinctive kinds of random number generator RC4 random number generator. After that discover how much time and energy is devoured by this convention. This work contains protocols which furnish secure and effective information transmission with least energy and time utilization so it makes it harder and hard to break the security of information. Investigations completed for all calculations utilizing MATLAB 7.8.***

Keywords: ***Wireless Sensor Network, MATLAB, Lightweight protocol, Dynamic key, RC4, Encryption, Decryption, Pseudo random number.***

I. INTRODUCTION

Security in a wsn is extremely important moreover; it should be reliably without interruption-

- Security requirements
1. Confidentiality
2. Authentication
3. Non-repudiation integrity
4. Integrity
5. Freshness
6. Forwards and backward secrecy
- Survivability requirements
1. Reliability
2. Availability
3. Energy efficiency

Cryptography Concepts:

- Cryptanalysis is a science of analysing cipher text to decrypt it and extract hidden information without the knowledge of encryption mechanism.
- Cryptography is a mechanism to provide the secure communication between two parties in the presence of third Party. Cryptography uses the modern mathematical theory and computer science approaches.
- Cryptology is the mathematics, such as number theory, application of formulas and algorithm that underpin cryptography and cryptanalysis.
- Plaintext: This is the original message file. All the encryption technique is applied over it.
- Cipher text: It is the encoded message of the original message. It is an unreadable form of the original message.
- Encryption: Encryption is the way to convert plaintext into cipher text. It take the two parameter one is key and another one is plaintext.
- Decryption: It is the way to convert cipher text into the original form of the message. It has two parameters one is the input key and another one is cipher text which we want to convert into the original message.
- Symmetric key: Only one key is used by sender and receiver for both encryption and decryption operation.
- Asymmetric key: In this two keys are used one for encryption and another is for the decryption. In this sender use one to perform encryption and another key is used for decryption.
- Key: Key is mainly used to provide the secure communication between two communication parties.

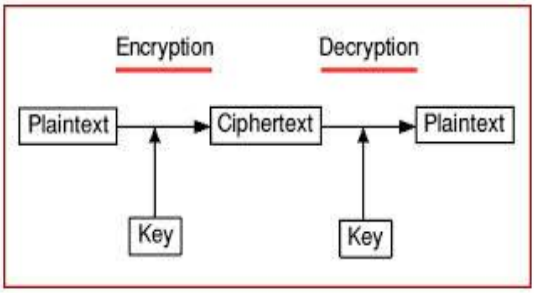

Fig 1. Encryption and Decryption process

Cryptography is probably the most important aspect of communication security and is becoming increasingly important as a basic building block for computer security.

The increased use of computer and communication systems by industry has increased the risk of theft of proprietary

information.
To avoid this one has to send the encrypted text or cipher.
Cryptography is now an emerging research area where the scientists are trying to develop some good encryption algorithm so that no intruder can intercept the encrypted message.
Based on application some of solutions for wireless sensor network security can be evaluated as follow:
(i) Different network architecture like distributed or hierarchical.
(ii) Key management such as pre-distributed or dynamically generated pair wise, group-wise or network wise keys.
(iii) Different styles of communication like pair-wise (unicast), group-wise (multicast) or network-wise (broadcast).

II. RELIABILITY OF WSN

1. Packet reliability:Packet reliability requires all the packets carrying sensed data from all the sensor nodes to be reliably transported to the sink.
2. Event reliability:event reliability ensures that the sink only gets enough information about a certain event happening in the network instead of sending all the sensed packets.

In addition to packet or event reliability; the successful recovery of certain event information can be reliably achieved either at hop-by-hop or end-to-end level.
Hop-by-hop: In hop-by-hop,, the next hop is responsible for ensuring the reliable transmission of information to the destination i.e. the sink node.
End-to-end:in end-to-end reliability, only the end points (i.e. only the source and destination nodes) are responsible for ensuring the successful transmission of information.

III. RELATED WORK

Antonio Damaso et al. [2], introduce the security of the wireless sensor network. Wireless sensor networks (WSNs) comprise of hundreds or thousands of sensor nodes with restricted preparing, stockpiling, and battery capacities. There are a few systems to decrease the power utilization of WSN nodes (by expanding the network lifetime) and increment the dependability of the network (by enhancing the WSN nature of administration).

It displayed a WSN dependability show that is produced naturally from the WSN topology and data about embraced directing calculations and the bit battery level. This model considers that WSN can bomb in two focuses: connections and sensor nodes.

This paper has three fundamental commitments identified with the assessment of WSN :it considers the bit energy level as the principle factor of disappointments of WSN nodes; it utilize the directing calculation to characterize the way between various WSN locales and the sink node; and it consequently creates unwavering quality models considering the previously mentioned components.

Muhammad Adeel Mahmood et al. [3], it is a review on existing information transport dependability protocols in wireless sensor networks (WSNs). The greater part of the current research utilizes retransmission systems to accomplish unwavering quality, disregarding the utilization of excess plans, for example, deletion codes to improve occasion dependability. We audit the information transport unwavering quality plans regarding occasion and parcel dependability utilizing retransmission or repetition instruments. Besides, we examination and think about the current information transport unwavering quality protocols in light of a few characteristics, uniquely the significance of occasion dependability over bundle dependability using retransmissions or excess. Based on the investigation, we at long last call attention to some future research bearings and difficulties ahead with a specific end goal to upgrade unwavering quality in WSNs.
In WSNs, dependability can be grouped into various levels i.e.

- Packet or Event unwavering quality level
- Hop-by-Hop or End-to-End unwavering quality level

To address the unwavering quality issue in sensor networks, we reviewed the different existing protocols that oversee information transport dependability and every one of them has its one of a kind method for guaranteeing dependability. Some of them require full end-to-end bundle unwavering quality while others can endure some level of parcel misfortune relying upon the idea of utilization they are taking a shot at. The most generally utilized systems to guarantee parcel or occasion unwavering quality incorporates the utilization of retransmissions component while others utilize data repetition to guarantee dependability. Jump by-bounce retransmission systems perform better when contrasted with end-to-end instruments in lossy situations, particularly when there is a high bounce tally from source to goal. The high jump check presents more passage focuses for mistakes which turn into the reason for bundle misfortune, in this way influencing unwavering quality. Bounce by-jump instrument performs better, as misfortune recuperation is performed at each middle of the road bounce from source to the goal. The jump by-bounce instruments can additionally be enhanced when it is performed for accomplishing occasion unwavering quality. Prerequisite of a dynamic retransmission timeout component and proficient support administration framework for forestalling stale bundles involving the line would be leeway to the current protocols with a specific end goal to spare sensors' restricted resources.

Paulo Rogerio Pereira et al.[4],Proven transport protocols like TCP, intended to help client applications in framework networks, normally display huge wasteful aspects when utilized without extensive alteration in WSN frameworks. One of the fundamental components for TCP insufficiency is connected with its entirely end-to-end unwavering quality model, constraining all affirmations and retransmissions to take after the total way amongst source and goal, with the ensuing toll on the officially rare bandwidth and energy. A few recommendations were made for elective transport

protocols, typically centered around particular improvement perspectives and/or application situations. Diverse WSN applications require distinctive evaluations of dependability. Correspondence protocols for WSN ought to be energy-productive to keep away from futile squandering of energy resources through minimization of the control and retransmission overhead; ought to have disseminated usefulness to misuse the WSN resources in helpful way, with the goal that general WSN activity isn't blocked by the constrained limits of individual Paulo Rogério Pereira et al. nodes; and ought to give dependability separation to help diverse unwavering quality evaluations keeping in mind the end goal to suit the necessities of various applications in regards to throughput, inactivity and energy utilization.

RC5 algorithm

RC5 uses 3 primitive operations and their inverses:

Addition modulo 2^w - +

XOR - $\oplus$

Left circular shift denoted by x<<<y, where word x is rotated y bits. Right circular shift is denoted by x>>>y.

Figure 6.6a depicts encryption:

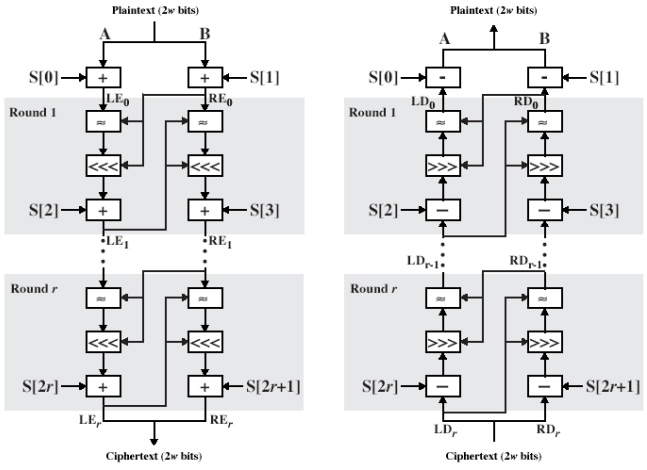

Fig 2 RC5 Encryption and Decryption

The plaintext is assumed to initially reside in the two w-bit registers A and B. We use variables LEi and REi to refer to the left and right half of the data after round i has completed. The algorithm can be defined as follows:

LE0=A+S[0];
RE0=B+S[1];
For i=1, r{
  LEi=((LE(i-1) $\oplus$ RE(i-1))<<<RE(i-1)+S[2i];
  REi=((RE(i-1) $\oplus$ LEi))<<<LEi+S[2i+1];
}

The resulting ciphertext is contained in LEr and REr. Note that both halves of data are updated each round.

Decryption

Decryption, shown in Figure 3.1 (b) , is easily derived from the encryption algorithm. In this case, the 2w bits of ciphertext are represented by LDr and RDr.

It use LDi and RDi to refer to the left and right half of data before round i has begun, where rounds are numbered from r down to 1:

For i=r downto 1{
  RD(i-1)=((RDi-S[2i+1])>>>LDi) $\oplus$ LDi);
  LD(i-1)=((LDi-S[2i])>>>RD(i-1)) $\oplus$ RD(i-1));
}
B=RD0-S[1];
A=LD0-S[0];

Analysis and Simulation of Proposed Work

The implementation of the proposed work is carried out in the MATLAB.

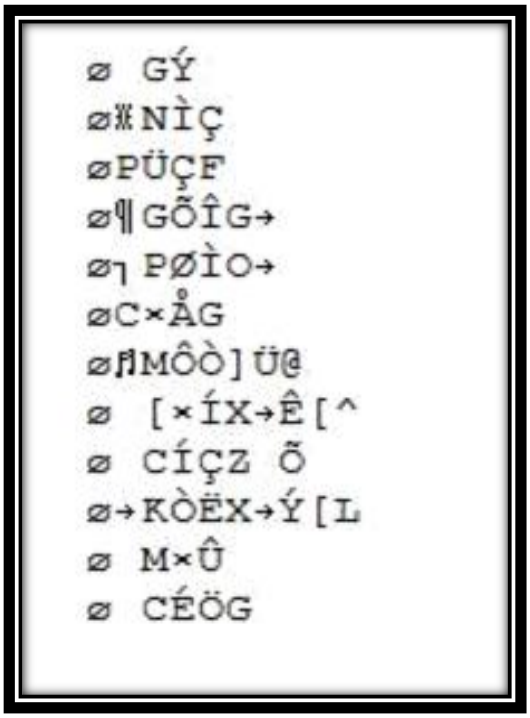

Fig 3 Key Generation

Fig 3 shows the key list obtained after the usage of the RC5 algorithm.

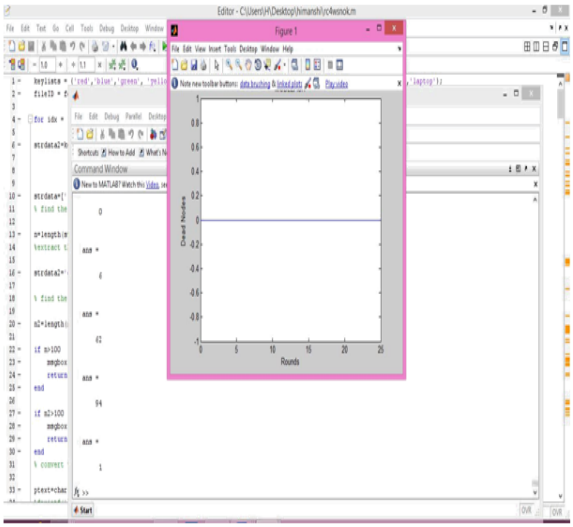

Fig 4 Dead Nodes after the Key Generation

Fig 4. Shows the dead nodes generation after the key validation is passed. And similarly other simulation related to the LEACH will be carried out performing the message sending in the Wireless Sensor Network.

Fig 5 shows the Key Generator 2 working which generates or simulates the hacker attacks using the invalid keys.

Fig 5 Key Generator 2

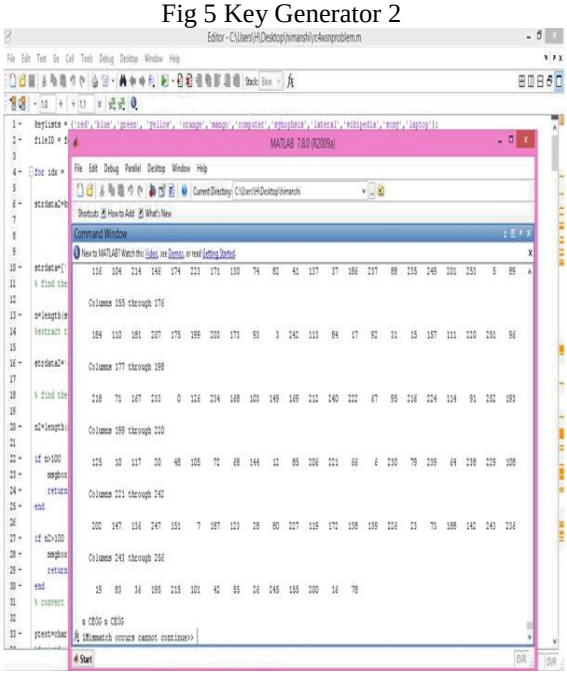

Fig 6 Mismatch data after key generator2

Fig 6 shows that in the key generator2 data cannot match, so we cannot use the wireless sensor network

IV. CONCLUSION

We store the key gave in each go in the 1-D cluster of string, in which every component is the key esteem. It is give the security of the wireless sensor network. In this encode the plaintext which is entered by the client by utilizing dynamic key than again decode the plaintext into the first type of the message. Anyway later if circumstance demands the task can be influenced fit for any wireless sensor to network and we add some new activities to made the convention difficult to break so it increment the security of nodes. It gives central security to wireless sensor network. In this venture, dynamic key administration systems have been utilized. Predominantly all the key administration plans are outlined in light of the constrained asset of sensor nodes and its security. Key Management plot for WSNs is as yet an extremely productive research bearing to be more found. The outcome hypothesis is invalid key is network which will show up when the rundown of keys contains the invalid key. The primary solid purpose of this strategy is dynamic key which produce each time after encryption and unscrambling process. It just uses RC5 for information transmission, key age and information validation in the proposed secure convention, so the hardware is anything but difficult to outline and deliver, and works with low power, handling and time costs. Likewise, considering most existing hardware supporting for RC5, the proposed convention ought to be perfect with existing hardware.RC5 stream figure is a productive cryptographic strategy for anchoring the information in a correspondence channel as it is less difficult and quicker than numerous different calculations..

REFERENCES

[1] William Stalling, “Applied Cryptography” 4th Ed.

[2] Dâmaso, Antônio, Nelson Rosa, and Paulo Maciel. "Reliability of Wireless Sensor Networks." Sensors 14.9 (2014): 15760-15785.

[3] Mahmood, Muhammad Adeel, Winston KG Seah, and Ian Welch. "Reliability in Wireless Sensor Networks: A Survey and Challenges Ahead."

[4] Pereira, Paulo Rogério, et al. "End-to-end reliability in wireless sensor networks: Survey and research challenges." EuroFGI Workshop on IP QoS and Traffic Control. Vol. 54. 2007.

[5] Tripathy, Somanath. "LISA: lightweight security algorithm for wireless sensor networks." Distributed Computing and Internet Technology. Springer Berlin Heidelberg, 2007. 129-134.

[6] Cai, Wenyu, et al. "Research on reliability model of large-scale wireless sensor networks." Wireless Communications, Networking and Mobile Computing, 2006. WiCOM 2006. International Conference on. IEEE, 2006.

[7] Zhang, Chang N., and Qian Yu. "An RC4 based Light Weight Secure Protocol for Sensor Networks." Wireless and Optical Communications. 2006.

[8] Kiruthika, B., R. Ezhilarasie, and A. Umamakeswari. "Implementation of Modified RC4 Algorithm for Wireless Sensor Networks on CC2431." Indian Journal of Science and Technology 8.S9 (2015): 198-206.

[9] Kim, Sukun, Rodrigo Fonseca, and David Culler. "Reliable transfer on wireless sensor networks." Sensor and Ad Hoc Communications and Networks, 2004. IEEE SECON 2004. 2004 First Annual IEEE Communications Society Conference on. IEEE, 2004.

[10] Katiyar, Mamta, H. P. Sinha, and Dushyant Gupta. "On Reliability Modeling in Wireless Sensor Networks-A Review." International Journal of Computer Science Issues(IJCSI) 9.6 (2012).

[11] Chen, Ing-Ray, and Yating Wang. "Reliability analysis of wireless sensor networks with distributed code attestation." Communications

Letters, IEEE16.10 (2012): 1640-1643.
[12] Song, Yongxian, et al. "Design and analysis for reliability of wireless sensor network." Journal of Networks 7.12 (2012): 2003-2010.
[13] Tripathy, Somanath. "LISA: lightweight security algorithm for wireless sensor networks." Distributed Computing and Internet Technology. Springer Berlin Heidelberg, 2007. 129-134.
[14] Jaggle, C., et al. "Introduction to model-based reliability evaluation of wireless sensor networks." 2nd IFAC Workshop on Dependable Control of Discrete Systems. 2009.

