To Provide Security Using Encryption and Compression Technique In WSN

A K Kadao[1], D V Jamthe[2], M S Chaudhari[3]
Department of CSE
[1]PG Student, Priyadarshini Bhagwati College of Engineering, Nagpur.
[2]Assistant Professor, Priyadarshini Bhagwati College of Engineering, Nagpur.
[3]Assistant Professorand Head, Priyadarshini Bhagwati College of Engineering, Nagpur.

Abstract-*The wireless sensor network consists of various nodes without any connection between them. These wireless sensor networks are in distributed form. Some researches explain that the data is distributed only from the base station. This is drawback of wireless sensor network. The wireless sensor network doesn't provide the security to the sensor nodes for transferring the data. When a rivest cipher and run length encoding techniques are provides for the security and compression purpose. So, the system will secure and it will take less time for transferring data. Again it can save a storage capacity.*

Keywords*-*RC6, RLE, Security, WSN

I. INTRODUCTION

There is important to improve the outdated small programs or parameters for storing in sensor nodes. The Wireless Sensor Network is a collection of large number of tiny low power, low cost and multifunctional sensor nodes. These nodes are randomly and highly distributed inside the system. The sensor nodes are small in size which consist the sensing unit, data processing unit and geographic positioning system and power supply units. The hundreds and thousands of sensor nodes are used by wireless sensor nodes. These sensor nodes are flexible and directly associate with the base station. Wireless sensor network provide the various information about different structures.

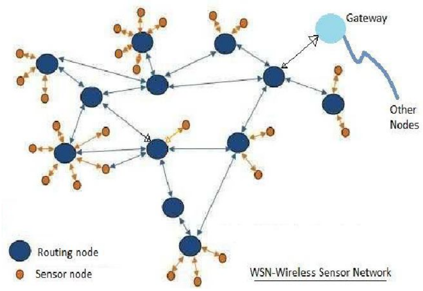


Fig.1 Dissemination of Data through Nodes

Figure 1 shows the data is disseminated through the various nodes to the proper destination by using the gateway. It containing the routing nodes and sensor nodes. This shows dissemination of data.

II. RELATED WORK

Some papers describe the various issues and related work. Shailesh N. Sisat, Prof.Shrikant J. Honade [2] gives the WSN security solutions, system architecture for communicating using WLAN and security requirements in wireless sensor network. The paper is concluded that data can be secure from malicious attacks and third parties. RC6 used for improving the reliability purpose. Swati Sharma, Dr. Pradip Mittal [5] describe the architecture and applications of WSN like military application, application, home and commercial applications. This paper showing the different routing protocols like SPEED, GAF, HBR, GEAR, LEACH etc. Finally the paper is concluded that routing protocol could be the consideration of node mobility. Wireless sensor network need to handle the overhead of mobility and topology changes in different conditions.

Aamir Sheikh, Siraj Pathan [6] describe the various things like fusion technology of WSN and RFID, IEEE820.15.4/zigbee protocol stack architecture and structure of the framework of remote monitoring system. Finally concluded thatwireless protocol in personal area have unique characteristics which are including low cost low data rate and low power consumption.

Kuthadi Venu Madhav, Rajendra C. and Raja Lakshmi Selvaraj [8] describe the unique characteristics of WSN and security challenges of WSN. Again the paper gives explanation of security mechanism. They concluded that WSN has unique characteristics, low cost deployment and real environment orientation. John Paul Walters, Zhengquiang Liang, Weisong Shi, Vipin Chaudhary [10] introduce the WSN. They gives the information about the sensor security obstacles and security requirements like data confidentiality, data integrity, data freshness, availability, time synchronization etc. Finally concluded that wireless sensor network is continuously growing and becoming more common.

III. IMPLEMENTATION

Rivest Cipher 6

RC6 is a part of cryptography. It is a symmetric key block cipher which derived from RC5. It has a proper size of 128 bits and supports key sizes of 128, 192 and 256 bits up to 2048 bits. Rivest cipher algorithm is simple, fast and secure. RC6 performs various operations like addition, subtraction, multiplication, bitwise exclusive and some rotations. It is fully parameterized family of encryption algorithm and more accurately specified as RC6-w/r/b. RC6 uses 4 bit register and more secure, compact and simple block cipher which offers flexibility and good performance.

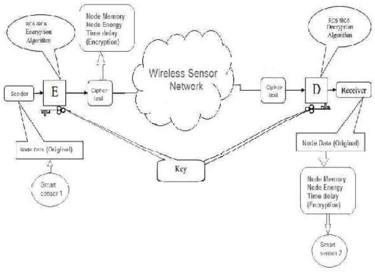

RC5/RC6 Encryption Algorithm
Node Memory Node Energy Time delay (Encryption)
Wireless Sensor Network
RC5/RC6 Decryption Algorithm
Sender
E
Cipher text
Cipher text
D
Receiver
Node Data (Original)
Node Data (Original)
Key
Smart sensor 1
Node Memory Node Energy Time delay (Encryption)
Smart sensor 2

Fig. 2 RC6 working

Figure 2 shows, the sender sending the confidential data. The senders don't want to receive the data other receiver. So sender is using the key E and original data is converted into the cipher text which is unreadable form for intruder. The receiver using the key D for the decryption purpose. The receiver will receive the data in unreadable form and will use key D for converting the cipher text into original form which will be readable.

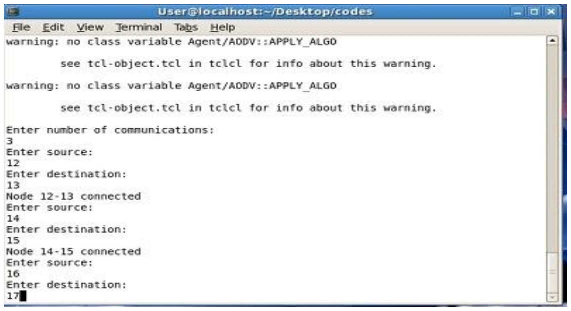
Run Length Encoding

Run Length Encoding is a very simple form of lossless data compression which is runs of data is stored. It is used for compressing any type of data and content of data will affect the compression ratio achieved by RLE. It works by reducing the physical size of repeating string of characters. After applying the run length encoding technique the data is compressed and flow of data is increased and is taken the less time of transferring the data. The purpose is to save the storage space and reduce communications capacity requirements. RLE can be used for any type of contents but the compression efficiency is changes significantly. It depends on which type of data is using.

IV. PROPOSED WORK

The nodes will create a network between them. So the nodes can be communicate each other and share the information with each other. Then the RC6 and RLE will be applied on the nodes. Then the nodes can be sharing the data more secure form. The run length encoding is using for the compression purpose. It will take the less time for sharing data and can save the storage capacity.

V. EXPERIMENTAL RESULT


User@localhost:~/Desktop/codes
File Edit View Terminal Tabs Help

```
warning: no class variable Agent/AODV::APPLY_ALGO

        see tcl-object.tcl in tclcl for info about this warning.

warning: no class variable Agent/AODV::APPLY_ALGO

        see tcl-object.tcl in tclcl for info about this warning.

Enter number of communications:
3
Enter source:
12
Enter destination:
13
Node 12-13 connected
Enter source:
14
Enter destination:
15
Node 14-15 connected
Enter source:
16
Enter destination:
17
```

Fig. 3 asking for networking

Figure 2 shows, it gives the instructions for entering number of communications, source and destination. There are 3 numbers of communications. There are 12, 14, 16 sources and 13,15,17 destinations.

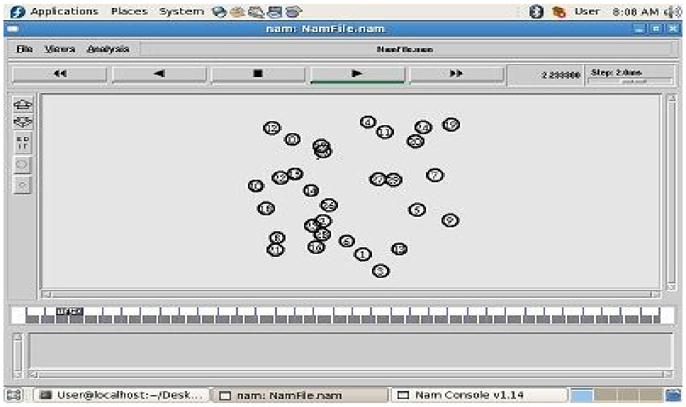
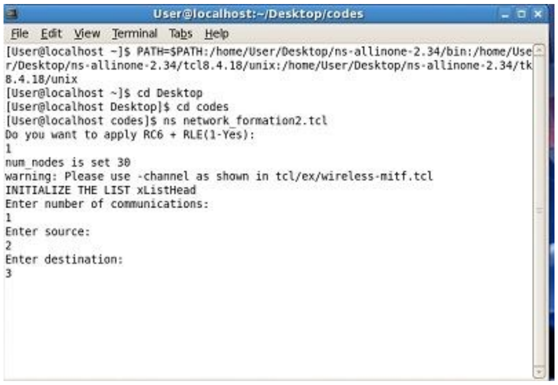


Fig. 4 nodes communication

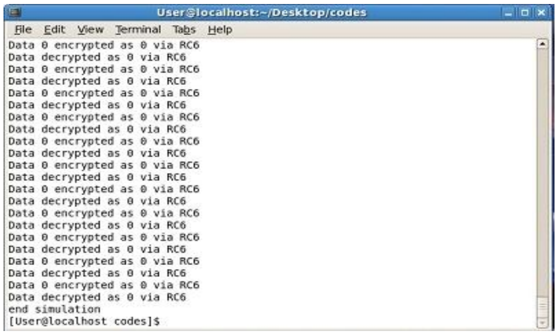
Figure 3 shows, there are 30 number of nodes. The above mentioned sources and destinations are communicating each other.


User@localhost:~/Desktop/codes
File Edit View Terminal Tabs Help

```
[User@localhost ~]$ PATH=$PATH:/home/User/Desktop/ns-allinone-2.34/bin:/home/Use
r/Desktop/ns-allinone-2.34/tcl8.4.18/unix:/home/User/Desktop/ns-allinone-2.34/tk
8.4.18/unix
[User@localhost ~]$ cd Desktop
[User@localhost Desktop]$ cd codes
[User@localhost codes]$ ns network_formation2.tcl
Do you want to apply RC6 + RLE(1-Yes):
1
num_nodes is set 30
warning: Please use -channel as shown in tcl/ex/wireless-mitf.tcl
INITIALIZE THE LIST xListHead
Enter number of communications:
1
Enter source:
2
Enter destination:
3
```

Fig. 5 asking for security and compression

Figure 4 shows, the system is asking for providing the RC6 and RLE techniques. RC6 is proving the security and RLE compress the data.


User@localhost:~/Desktop/codes
File Edit View Terminal Tabs Help

```
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
Data 0 encrypted as 0 via RC6
Data decrypted as 0 via RC6
end simulation
[User@localhost codes]$
```

Fig 6 data in encrypted & decrypted form

Figure 5 shows, the data is in the encrypted and decrypted form. So, the communication between the nodes will be more secured.

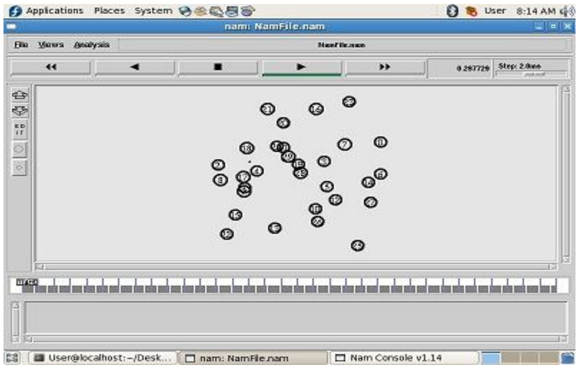


Fig. 7 communication in secured form

Figure 6 shows, the nodes are communicating in secure form and compress form. So the more data can be store in less time.

VI. CONCLUSION

The wireless sensor network area is growing day by day. The nodes are communicating without using any cables. The communication between nodes is start by creating the connection between them in WSN. The RC6 and RLE both are applied for some purpose. RC6 is used as a encryption decryption technique and RLE is used for the compression purpose. The RC6 and RLE both techniques are successfully used and worked.

REFERENCES

[1] M.Padma, T.Veeraju, ”A New Protocol For Mitigate Attacks And Efficient Data Forwarding In WSN”, in International Journal Of Computer Science And Technology, Volume 7, Issue 4, Oct-Dec 2016.

[2] Shailesh N. Sisat, Prof.Shrikant J. Honade, “Security and Privacy in Wireless Sensor Network Using RC6 Algorithm”, in International Journal Of Advanced Engineering Research And Science, Vol-3, Issue-5, May 2016.

[3] Shristi Bhute, Sddhartha Kumar Arjaria, “An Efficient AES and RC6 Based Cloud User Data Security With Attack Detection Mechanism” in international journal of advanced technology and engineering exploration, vol.3, 2016.

[4] Ms. K.Arul Keerthi, Ms. M.Shirin Ayisha Maryam, ”Increased Security And Distribution Using Didrip Protocol In Wireless Sensor Networks” in Sixth International Conference On Emerging Trends In Engineering And Technology, 2016.

[5] Josie Hughes, Jiz Yan and Kanchi Soga, “Development Of Wireless Sensor Network Using Bluetooth Low Energy (BLE) For Construction Noise Monitoring”, in International Journal On Smart Sensing And Intelligent Systems, Vol.8, No.2, June 2015.

[6] Pardeep Kaur, Vinay Bhardwaj, “Wireless Sensor Network: A Survey”, in International Journal Of Advanced Research In Computer Science And Software Engineering, Vol.5,Issue 5, May 2015.

[7] Swati Sharma, Dr. Pradip Mittal, “Wireless Sensor Networks: Architecture, Protocol” in International Journal Of Advanced Research In Computer Science And Software Engineering, Vol.3, Issue 1, January 2013.

[8] Aamir Sheikh, Siraj Pathan, “Research On Wireless Sensor Network Technology”, in international journal of information and education technology, Vol.2, No.5, October 2012.

[9] Nitin Mittal, Dawinder Pal Singh, Amanjeet Panghal, R.S. Chauhan, “Improved LEACH Communication Protocol For WSN”, in National Conference On Computational Instrumentation CSIO Chandigarh, India, March 2010.

[10] Kuthadi Venu Madhav, Rajendra C. and Raja Lakshmi Selvaraj, “A Study Of Security Challenges In Wireless Sensor Network”, In Journal Of Theoretical And Applied Information Technology, 2010.

[11] Chiara Buratti, Andrea Conti, Davide Dardari and Roberto Verdone, “an overview on wireless sensor networks technology and evolution”, in sensors, 2009.

[12] John Paul Walters, Zhengquiang Liang, Weisong Shi, Vipin Chaudhary, ”Wireless Sensor Network Security: A Survey” in Security In Distributed, Grid And Pervasive Computing, 2006.