To Secure DiDrip Protocol using RC6 and RLE in WSN

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

Abstract— The WSN consists of distributed nodes which support for sensing, signal processing, embedding and connectivity. The configuration parameters of sensor nodes are updated and distributed by using a data discovery and dissemination protocol. The commands are managed to the sensor nodes for distributing the data. The data discovery and dissemination protocols are based on the centralized approach and data is distributed through the base station. The protocols are not designed with the security, so can be easily launch attacks and harm the network. There is need to provide a security to protocol. Hence, there is using the encryption algorithm for the security and confidentiality purpose. After applying the algorithm, the DiDrip is provably more secure and shows the high efficiency for the network. Rivert Cipher is applying to provide a security and encoding technique is used for the compression purpose. So the system will take less time for transferring the data. That means, the data will secure and confidential at the time of data distributed and dissemination on the sensor nodes.

Keywords: RC6, RLE, WSN

I. INTRODUCTION

The Wireless Sensor Network is a group of spatially concentrated and dedicated sensors which are used for monitoring and for keeping the record of physical conditions of the environment. The collected data is organized at central location using the wireless sensor network. By using the wireless sensor network can be update the old programs on the sensor nodes. The sensor nodes distribute the data and disseminated various data on nodes with the help of wireless channels. Wireless sensor network use the control information and command which may used for calling query information about the nodes which are available in networks. The data is collected from the main location, it is a base station. The base station also can say the centralized location.

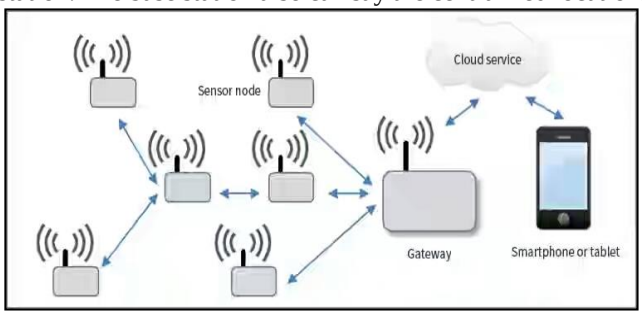

Fig. 1: Data distributing through WSN

The figure 1 shows that, the wireless sensor network included the more number of sensor nodes, gateway and smart phone or tablet. These are used for transferring data by using cloud services through the gateway. The wireless sensor network work in the environmental conditions like temperature, sound, pollution levels, wind speed and direction, pressure etc. Initially the wireless sensor network was used for only military operations but nowadays it is using in health, traffic and industrial areas. Generally, the sensors in WSN have a variety of purposes, functions and capabilities.

II. OBJECTIVES

1) To provide a security for data discovery and improve the confidentiality.
2) To increase a packet delivery ratio and reduce the dissemination time.
3) The user should send the data directly to the sensor nodes without using base station.
4) To deliver a piece of data to every node which allow by the administrators for reconfi-guring, querying and reprogr-amming a network.

III. DIDRIP

DiDrip satisfies the security requirement of the protocol. The DiDrip protocols have the four phases which are used for the flowing of information from the various states like Network Owner, Network User and Sensor Node.

A. Network Owner:

The DiDrip protocol allows network owner for authorizing the network user. It manages all networking related to protocol and it accepts the various formats from the network user and gives the permission the permission to the network user for transferring and receiving the data. The network owner is present in two phases like system initialization phase and user joining phase. That means the network owner is start from this phase.

B. Network User:

The network user uses the various formats which are provided by the network owners. Before transferring or receiving the data, the network users have to register to the network owner. After registering, the network user can be transfer and receive the data. The network users contain the packet preprocessing phase. In this the processes are preprocessing with the data and nodes.

C. Sensor Node:

The node in sensor network which is capable of performing some processing, gathering information and communicating with other nodes, is called sensor node. These nodes are used for verifying the packets which are transferring by the network user. Sensor node is present with the packet verification phase. In this phase, the packets are verified by the nodes and after that the packets can be transfer and receive by the system.

All rights reserved by www.ijsrd.com

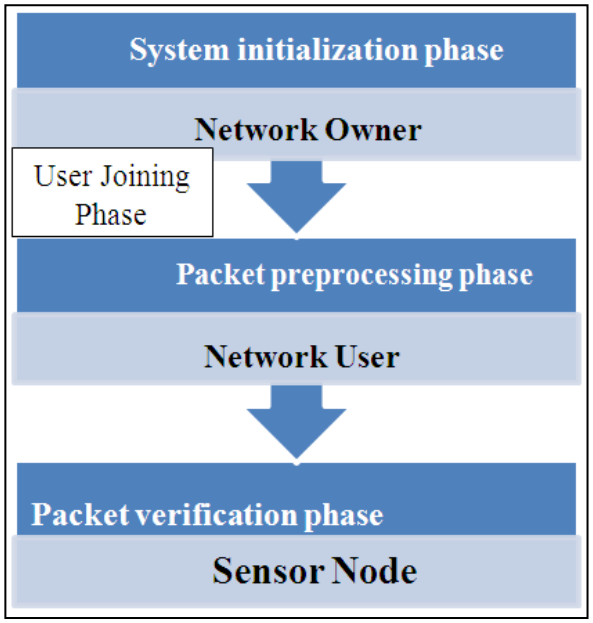

Fig. 2: Information Processing Flow in DiDrip

Figure 2 shows the various stages for flowing of information by using the phases.

IV. Requirements & Design Consideration

A. *Requirements:*

There are some requirements which are important for the DiDrip protocol.

B. *Expandable in Nature:*

The permission should be given to multiple network users for transferring the data over network without using the base station.

C. *User Concession:*

The network owner should be given various concession level to multiple users. These levels sets by network owner and should be support to multiple users by protocol.

D. *Authorized User:*

The protocol should be provide authenticate data to the only authorized user. The data can transfer to sensor nodes from the authorized user.

E. *Integrity of Data:*

The data should not be modified at the time of transferring data at network.

F. *Scalability:*

The protocol should work with thousand of nodes in WSN.

G. *Dynamic Network:*

The sensor nodes should be added to the network dynamically.

H. *Design Considerations:*

Generally, the sensor nodes consists the energy in limited form and capabilities for computation & storage the data. Most of the times, use the digital signature for the security purpose and provide the authentication to the data. But this approach is verify the signature at the time of transferring the data. Sometimes uses the symmetric key cryptography but it is not the safe at the time of communication or transferring the data. Merkle Hash Tree uses with digital signature and Elliptic Curve Cryptography technique for the purpose of security. By using the encryption technique the integrity is provide to the disseminated data. There is need to register on network owner by network user for receiving and transferring the data. The network owner issues the certificates by using public key infrastructure (PKI). The attack should be on sensor nodes by attacker and these attack can be internal or external attacks. So, the data should be infect in the network.

V. Proposed Work

The researchers uses the DiDrip protocol for data dissemination and security. The work can be improved by using RC6 algorithm for security purpose. But the system is taken more time for transferring the data that mean system get delay, so should be reduce the delay of the system. Hence there is using compression technique like RLE. Before encryption the data will compress and flow of data will be increase. Generally, the security technique is used for authenticity, integrity and confidentiality for the disseminated data items in DiDrip.

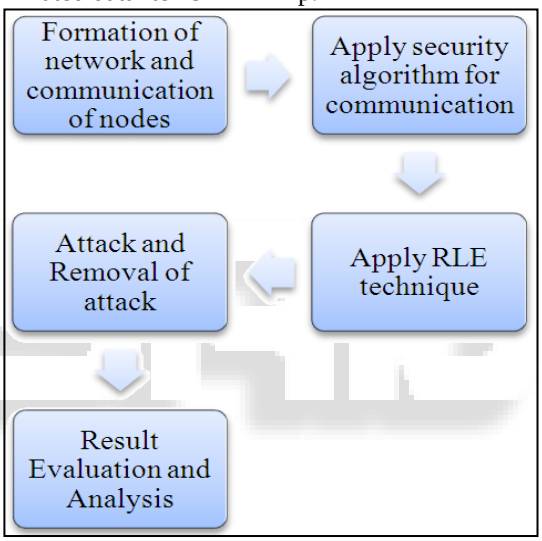

Fig. 2: Implementation of Proposed Work

VI. Experimental Results

A. *Communication between nodes:*

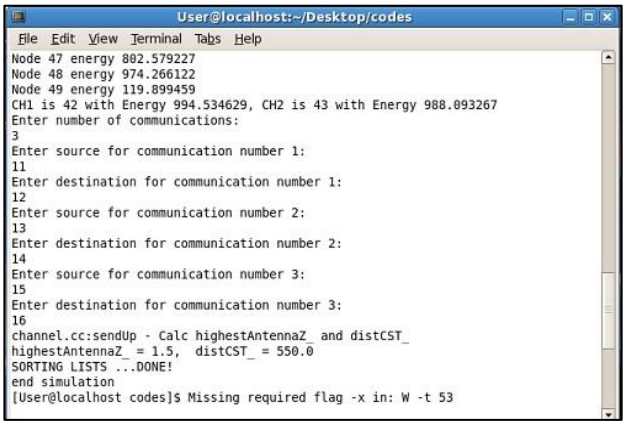

Fig. 3: Instructions given to system

The figure 3 shows, here the number of communications are entered. There are three numbers of communications. Here the nodes 11 and 12, 13 and 14, 15 and 16 are created the network between them.

All rights reserved by www.ijsrd.com

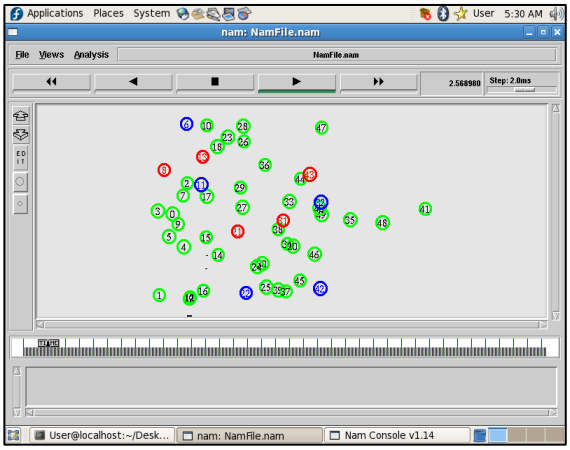

Fig. 4: Communication between nodes

The figure 4 shows, the network is created between the nodes. The nodes 15 and 16 are communicating with each other. There is communication without any security and without any compression technique.

B. Communication With Dissemination:

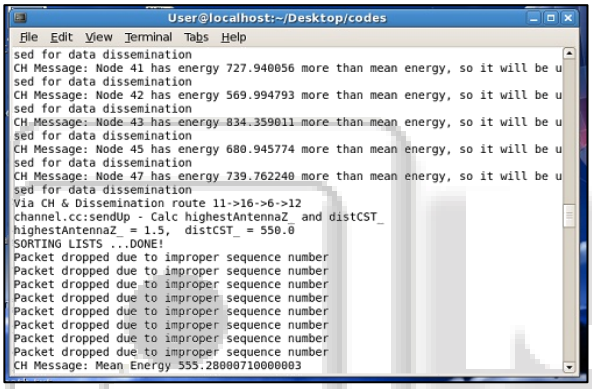

Fig. 5: creation of route

The figure 5 shows, the data dissemination is applied on the nodes and so the route is created between nodes for sharing data. The figure shows the route is created like 11-16-6-12.

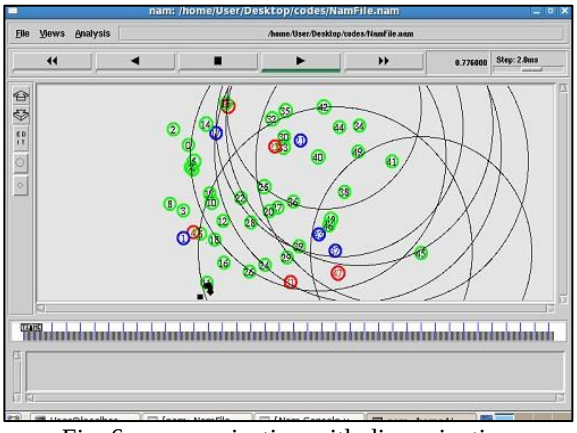

Fig. 6: communication with dissemination

The figure 6 shows, the packet is dropped due to improper sequence number and data is going from node 11 to 12 by creating a route. But there are chances of interfering by the intruder or stealing the data at the time of transferring the data.

C. Communication With RC6 and RLE:

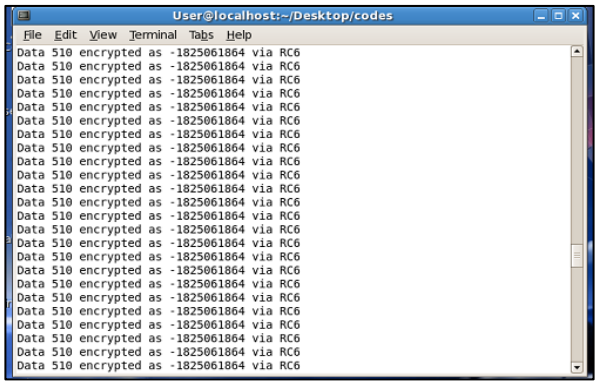

Fig. 7: data in encrypted form

The figure 7 shows, the RC6 and RLE is applied on the nodes. So the data is secured and in compress form. After compressing the data, it takes less time for transferring data and the data is also in encrypted decrypted form.

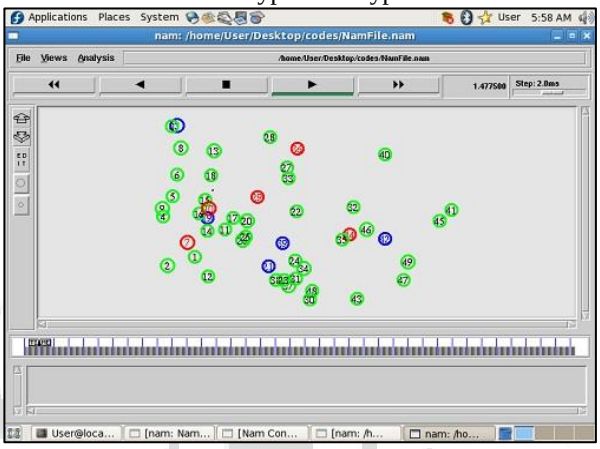

Fig. 8: communication in secured form

The figure 8 shows, the communication between the nodes 11 and 12 is in secured form. Here the RC6 is applied for security purpose, so the data is transferred by the source in encrypted form. Then the destination is received the encrypted from data and decrypt that data in original form. The nodes 11 and 12 are communicating in encrypted form.

D. Removal of Attack:

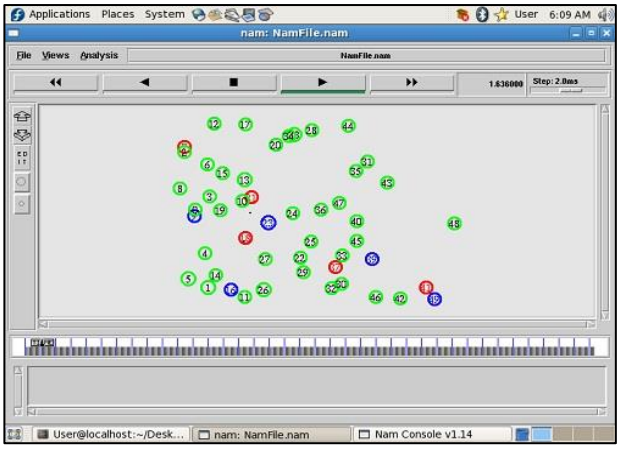

Fig. 9: Secured communication

The figure 9 shows the data dissemination is applied with the encryption and compression technique. Here the encryption technique is RC6 and compression technique is Run Length Encoding. The data is transferred in secured form and it saved storage space also because of RLE.

All rights reserved by *www.ijsrd.com*

E. Result Evaluation and Analysis:

50/3	De	E	J	PDR	TP
N	0.00109	3.402	0.00039	98.85	201.7
A	0.00087	10.32	0.00041	99.75	202.9
Di	0.00085	6.59	0.00006	99.61	214.3
DA	0.00079	3.16	0.0005	99.17	177.7

Table 1: Result Evaluation

Table 1 containing the some parameters like Delay, Energy, Jitter, PDR (Packet Delivery Ratio) and Throughput. The system has 50 nodes and the result showing for three communications. The result is shown for Normal(N), with algorithm (RC6+RLE), Dissemination(Di), Dissemination and algorithm (DA). This result is shown in the tabular format.

The figure 10 shows, the energy, delay and throughput is low after applying the data dissemination and algorithm as compared to other. The packet delivery ratio continuously changes and the value of jitter is also change. The value of jitter is depend on the problem occurred in the hardware.

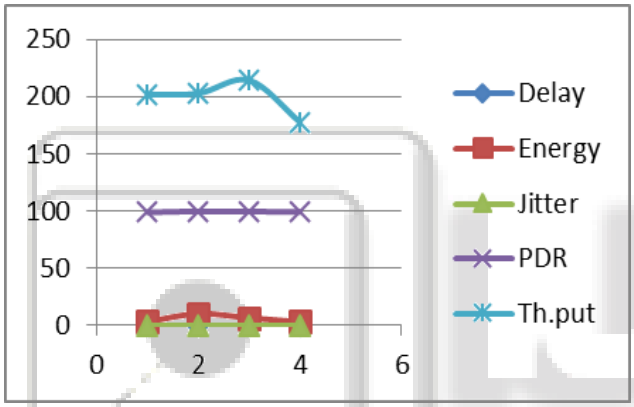

Fig. 10: Result Analysis

VII. Conclusion

The wireless sensor network is a wide and open area. The discovery and dissemination protocols are worked with wireless sensor network. From the study, we identified the security vulnerabilities in data discovery and dissemination. The survey work is done on the existing system of data distributed and dissemination protocols. The network is formed between the nodes and communicated with each other. The data dissemination is applied on the nodes. Then it creates the proper route for transferring the data. When the RC6 block cipher is applied on the nodes, the communication is more secured and compact which offers the good performance and flexible. The run length encoding technique is used for compressing the data. So it has taken less time for transmission of data. The data is compressed and the speed of flow of data increased. So the system had used less energy at the time of transferring the data from one to another. After applied encryption technique the chances of attack by intruder is decreased. So the data is more secured and is provide the confidentiality. So the intruder couldn't interfere at the time of data transferring and reduced the chances of stealing of data.

References

[1] P. Lakshmi Durga, Y. Yesu Jyothi, "*A Novel DiDrip Protocol with Dissemination Privilege Pair Authenticaion*" in Internattional Journal of Science Engineering and Advance Technology, Vol.5, Issue 1, January 2017.

[2] Dr.K.SureshBabu, G.SukeshBabu, "*Disseminate Authenticity and Integrity Data in Wireless Sensor Networks by using Secure DiDrip*" in International Journal of Professional Engineering Studies, Vol.VII, Issue 3, October 2016.

[3] B. Kiranmai, G. Sumalatha, "*Secure Data Propagation and Renovation of Nodes in Wireless Sensor Networks"* in International Journal & Magzine of Engineering Technology, Management and Research,Vol. No. 3, October-2016.

[4] Gouthami Bhandekar, Mrs.A.Naveena, "*Pre-rectification Technique- The Node Recovery for Secure and Distributed Data Dissemination in WSN*" in International Conference on Latest Innovation in Science, Engineering and Management, October 2016.

[5] M.Padma, T.Veeraj, "A new Protocol for Migrate Attacks and Efficient Data Forwarding in WSN" in International Journal of Computer Science and Technology, Vol.7,Issue 4, Oct-Dec 2016.

[6] Shobhna Vedprakash Pandey, Dr. K.Srujan Raju, "*DiDrip A Secure and Distributed Protocol for Updation and Dissemination of Data in WSN*" in International Journal of Advanced Engineering Research and Science, Vol.3, Issue 9, September 2016.

[7] Mamata, Deepak Biradar "*Ensuring Secure Communication By Providing High Security and Confidentiality in Wireless Sensor Networks*" in International Journal of Innovative Science, Engineering and Technology, Vol. 3, Issue 8, August 2016.

[8] Geeta, Shridevi Soma, "*Performance Analysis of Secure Data Distributing in Wireless Sensor Networks*" in International Journal of Advance research Foundation, Vol.3, Issue 6, June2016.

[9] Neha Dhotre, Prof. Ramesh Jadhav, "*A Multi Owner-Multi User Data Transmission for Secured Information in Wireless Sensor Networks*" in International Journal for Innovative Research in Science and Technology, Vol.3, Issue 1, June 2016.

[10] Aneesa Fatima, Gururaj Nase, "*An Efficient and Secure Data Dissemination Protocol for Wireless Sensor Network"* in International Journal of Combined Research & Development (IJCRD), volume: 5, Issue:6, June-2016.

[11] Dr. G. Venkata Rami Reddy, B. Syamala, "Data Detection and Distribution in WSNs by Using DiDrip Technique" in International Journal of Research In Advanced Engineering Technology, Volume 5, Issue 3, May 2016.

[12] Pattanashetti Vijay Iranna, B.N.Veerappa, "*Secure and Discovery of Distributed Information and Spreading in Wireless Sensor Networks*" in International Journal of Innovative Research in Computer and Communication Engineering, Vol. 4, Issue 5, May 2016.

[13] Pragya Kataria, Prof.R.K.Krishna, "*A Survey on Data Confidentiality for Providing High Security in Wireless Sensor Networks*" in International conference on Science

All rights reserved by *www.ijsrd.com*

and Technology for Sustainable Development, May 2016.

[14] Savitri, Sheela Shridhar, "*Distributed and Secure DiDrip Protocol for Data Discovery and Dissemination in WSNs",* in International Journal of Innovative Research In Science, Engineering and Technology, Vol. 5, Issue 4, April-2016.

[15] Indermohan Singh Major, Dr. R. S. Kawitkar, "*Mechanism of Secure and Distributed Data Discovery and Dissemination in Wireless Sensor Networks",* in International Journal of Innovative Research in Computer and Communication Engineering, Vol.4, Issue 3, March-2016.

[16] Shruthi K, Binoy Panicker, "*Sec-DiDrip: A Distributed Data Dissemination Protocol with Enhanced Security*" in International Journal of Advanced Research in Computer and Communication Engineering, Vol.5, Issue 1, February 2016.

[17] Yadavalli Devipriya, Potluri Avinash, "*Secure Data Detection and Distribution in WSNs Based on AES and DiDrip Techniques*" Vol.5, Issue 3, 2016.

[18] Ms. K. Arul Kirthi, Ms. M. S. Shriin Ayisha, "*Increased Security and Distribution Using DiDrip Protocol in Wireless Sensor Networks*" Sixth International Conference on Emerging Trends in Engineering and Technology, 2016.

[19] A. Senthil Kumar, S. Velmurugan, Dr. E. Logeshanmugan, "*A Secure Distributed Data Discovery and Dissemination in Wireless Sensor Networks",* in International Journal of Engineering & Science Research, Vol-5/Issue-7/708-713, July-2015.

[20] Raja Rajeswari T S, Manjunath K G, "*Robust and Efficient Protocol to authorize Multiple Network Users in WSN*" in IRF International Conference, Bengaluru, May 2015.

All rights reserved by *www.ijsrd.com*