International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.06, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

Approved Node with Enhanced ECC Approach for Effiecent transmission in Wireless Sensor Network

Kumari Ravneet[1], Arshdeep Singh[2]

[1]Student Department of IT, A.I.E.T Faridkot,Punjab
[2]Asst. Professor Department of CSE, A.I.E.T Faridkot,Punjab

ABSTRACT

The wireless network sensor includes a wide range of scenarios. In one of these networks, the network consists of a large number of nodes in a large area where not all nodes are directly connected. The exchange of data is supported by multi-hop contacts. The sensor node has a limited range, processing and storage capacities, as well as its limited energy resources. The WSN-MCC combination model used as data source for users of the cloud and mobile devices data for the cloud. With reliable user and devices can obtain the sensory data required from the cloud, where and when there is a network communication Wireless sensor networks play an important role in our lives, so they need to be safe. The basic principles of wireless sensor network and code deployment technology is introduced the effect of data transmission in WSN-MCC on the network at the same time is monitored. The technique called Enhanced ECC with Approved nodes to make the data transmission effective.

Keywords

Wireless sensor network, Elliptic curve cryptography, Approved Node.

1. INTRODUCTION

The networks of wireless sensors are formed by several nodes that act to denote the data working data and pass information between them through wireless communication. [1] Each sensor node is equipped with several devices such as microcontroller, radio, receiver, antenna and microcontroller. Tendency to detect the data and the exchange of data between the nodes of the network. [4] Network applications vary from military surveillance to forest fires and security monitoring, which makes them very important and valuable. In the global military networks they transmit confidential information that must be protected from intruders and attackers and N is a big problem [2].

To get data from the power, age, data storage and processing power of a powerful MCC to bring revolution to today's industry for more attention. The main idea of MESN integration is to use powerful sensors in wireless sensor networks to collect data from the environment and store it on a powerful server on the platform. This sensory data is processed and then transferred to sensory data that is processed for mobile phone users when they request it. In this integration, the sensor collects data from the network and sends it to the sensor door. When the sensor door receives the sensor data and processes the data and sends it to the cloud. The data is then processed and stored on the cloud. These data can be accessed by mobile users anytime, anywhere. WSN serves as a data source for cloud users and mobile data providers for the cloud. As a data source for consolidations, it's easy for mobile users to access environmental information and other necessary information by simply interacting with the cloud.

1.1 Architecture of WSN-MCC

This model is a combination of WSN-MCC, Wireless Sensor Network as a data source for cloud and mobile users are data sublicenses for cloud. With humble customers only on their mobile devices, mobile users can access the sensory data required from the cloud, wherever and whenever there is a network. The following diagram illustrates the integration framework of the multiple focal point. In this form, sensor networks can be composed of many different types of sensors, such as seismic, thermal, infrared optical, low-frequency magnetic, acoustic and radar sampling. These sensors can monitor a wide range of weather conditions such as weather, humidity, movement, temperature, pressure and housing information within a given area. Sensory data collected first is sent to the cloud for processing and storage. The cloud then sends this data to mobile users when requested upon request. The integration of the World Meteorological Organization (WAN-MASK) has led to a number of effective applications such as disaster detection, agriculture, irrigation control, transportation, real-time visualization of vehicles, monitoring of tunnels, monitoring of health care.

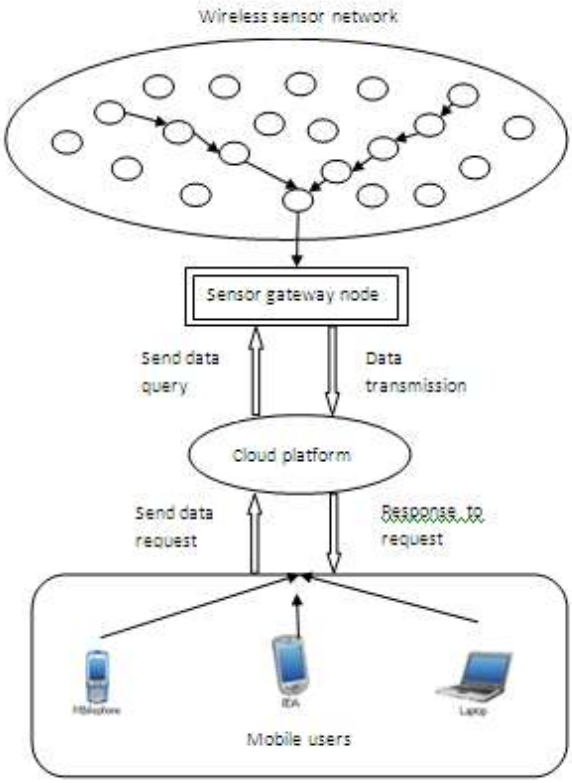

Fig 1: Architecture of a WSN-MCC

1.2 Elliptical Curve Cryptographic in Wireless Sensor Network

Elliptical Curve Cryptographic (ISK) is a public key cryptography technique based on elliptical curve theory that can be used to create faster, smaller, and more efficient cryptographic keys. [3]

Victor Miller and Neil Koplitz introduced an elliptical curve encoding in 1985. The spread of the elliptical curve encoding is due to the fact that it is located in a more complex mathematical problem than other cryptographic systems. It is an option that contradicts a routine open cryptographic key system, for example, RSA, DSA. It provides a similar level of security with a small size and enhances better execution in limited situations such as mobile phones, sensor management and smart cards. Elliptical Curve Cryptographic helps create equivalent security with less computing power and use of battery resources, and is widely used for mobile phone applications. [3]

Elliptical Curve Cryptographic got the attention of scientists because of its small size and provides possible results for practical implementation of the tools from the necessary resources. The previous work shows that open key calculations are a decent decision to use in the remote sensing network, and that the advantages of the ISK keys and recommendations will be critical to improving energy protection. ISK is used to achieve authentication and key management. The ECC has some related work on the age-dependent procedures that encode the elliptical curve. [3]

2. RELATED WORK

The author describes in [2] the new plan for the integration of satellite-based networks (SunSec) called TBS, which consists of two main parts: the first is the transfer of selective data based on time and priority (spread) so that the wireless sensor network sends more useful and reliable data to the cloud The second is the sleep-based priority programming algorithm (BS) to provide power consumption. Includes time and priority functions to improve the usefulness of sensory data, reliability and age. It is used to be permeated by gate and age to selectively transmit the sensor data which is most useful for the cloud. It is used by BC and Sun to provide power consumption for data collection and transmission, resulting in a more reliable operation. It takes both the PSTN and PST and the priority characteristics of the data required by the mobile user.

The data-processing framework for Wansen-Mesk proposed by the author in [3]. This framework analyzes the concept of wireless sensor network and mobile cloud computing. This main goal of the framework is to transfer the required data to mobile phone users in a faster, more reliable and secure way. This framework has worked on the problems of data transmission and storage in the mobile sensor network. This framework reduces storage requirements for sensory data nodes and the network gateway. It also reduces the excess traffic and network bandwidth requirements of the mobile sensor. This framework ensures that mobile users get the required data more quickly.

The delivery model uses three-phase security problems and threats in wireless communications and sensor network in [4]. The objective of this model is to analyze the cloud-based environment for wireless communication and the application of the sensor network along with the security problems of data management. The model is based on a three-stage decision-making process. Each organization moves towards cloud computing and Sun, in the form of a provider or consumer. Algorithm and three-phase data security method used to reduce threats and other problems in the cloud wireless network.

3. PROPOSED METHOD

3.1 Approved Node Formation

This work focuses mainly on improving the secure transport network for code distribution. In this system, some nodes are separated and these node nodes are called supported. These nodes are placed with the system nodes and are always placed around the code distribution environment. The main function of the node (receiver node) is to receive the service request from the network nodes

You will find the approved contract that is called the contract awarded (n) the following path of the approved nodes for a secure routing path. The network will generate a way to transfer messages securely; the message will be transmitted with encryption technology and all messages will be encrypted and transferred to the track flow. If the network fails between transmissions, you will begin to resend the code from the last granted node stored in the way the submission was suspended instead of starting a transition from the initial position.

ALOGRITM: Proposed technique

1: By time = 1 time simulation

2: For i = 1: N, where N is the number of nodes placed in the grid

3: Master: N, number of assigned nodes

Inside the path

4: Find the ID number n

5: If the site (i) is within the site (n).

6: Approved Node (An Id); store the information from the successive grant node in the path

7: Final IF

8: End

9: End

10: System End

4. Result and Discussion

1 Usefulness of Sensory Data: Sensory data utility: Figure 1 shows the comparative statement of 10 points in the utility of the sensory data of the prior art which decreases as code redistribution increases. This is due to the increase in any of the mobile phone users. If the redistribution suspension network with encryption is found throughout the network, the usefulness of the sensory data increases. However, the APN proposed to avoid such a situation by reducing the process of redistribution and encryption using the technique of sent nodes (era) a proposed technique to redistribute the code in the last supported node from which the network was suspended. As a result, our proposed technique shows a better result compared to the previous technology.

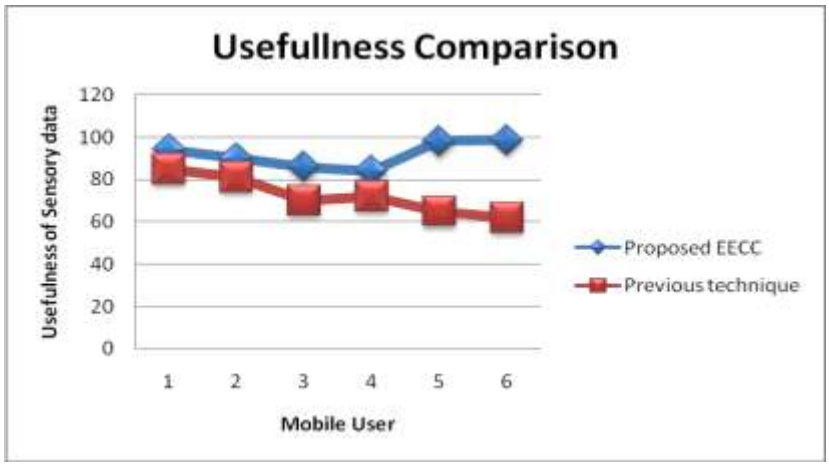

Fig.1 Mobile User vs. usefulness of Sensory Data

Table I Mobile user vs. Advertising Time comparison

Mobile user	Proposed EECC	Previous Technique
1	94	85
2	90	81
3	86	70
4	84	72
5	98	65
6	98.7	62

2 **Reliability of WSN**: Figure 2 shows the comparative implementation of the decade, namely the reliability of time (s) in the case of prior art. Decreases with increased redistribution of code. Due to the increase in the contract. Our proposed technology shows a better result than before, since in our proposed technology, the code redistribution is performed in the last given node rather than the entire network.

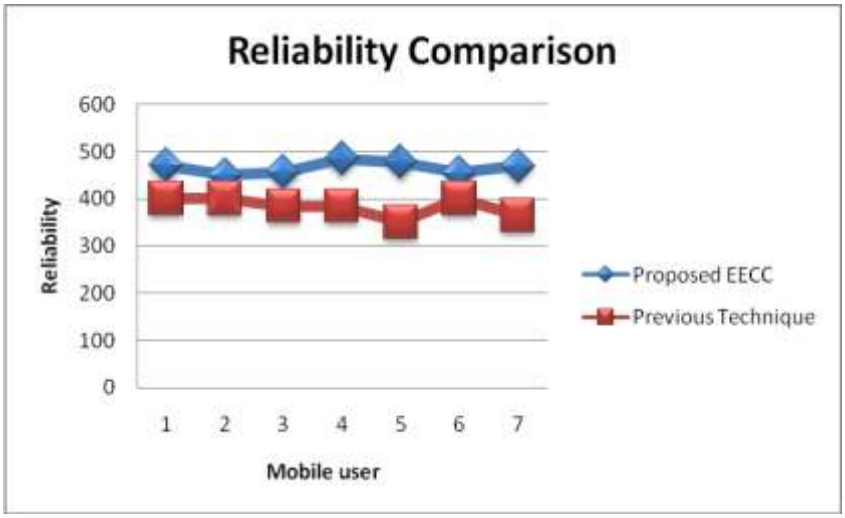

Fig 2 Mobile user VS of Reliability of WSN(hour)

Tabel 2 Mobile user VS of Reliability of WSN

Mobile user	of Reliability of WSN(hour)	
	Proposed EECC	Previous Technique
1	470	400
2	450	401
3	456	385
4	485	385
5	478	350
6	455	401
7	469	365

5. CONCLUSION

Deployment node is used to distribute Data using Approved node, the network consumes more power, so Approved uses improved data protection with minimal power usage in the nodes. It provides more reliability to data transmission, including protecting the integrity of the data. Proposed Technology provide security with ECC using approved nodes while transmission. The approved nodes provide route path in WSN-MCC integration Environment for reliable transmission.

.REFRENCES:

[1] Mrs. B. Chithra, Depavath Harinath,P.Satyanaryana, M.V Ramana Murthy, "Enhancing Security by using ECC Algorithm in Wireless sensor network", IJAIM, Volume-4, Issue1,ISSN 2320-5121, 2015.

[2] Himani Chawla,"Some issues and challenges of Wireless Sensor Networks", Volume 4, Issue 7, July 2014.

[3] Sangwon Hyun, Peng Ning, An Liu North Carolina State University Wenliang Du Syracuse University," Seluge: Secure and DoS-Resistant Code Dissemination in Wireless Sensor Networks", https://discovery.csc.ncsu.edu/pubs/ipsn08-seluge-IEEE.pdf.

[4] Asha Ran Mishra, Mahesh Singh, "Elliptic Curve Cryptography for Security in wireless sensor network", IJERT, ISSN: 2278-0181, Vol-1 issue 3, May-2012.

[5] Xiaoyang Zhong, Miguel Navarro, German Villalba, Xu Liang, Yao Liang, "MobileDeluge: A Novel Mobile Code Dissemination Tool for WSNs", *Mobile Ad Hoc and Senor Systems (MASS) 2014 IEEE 11th International Conference on*, pp. 537-538, 2014.

[6] Jian-Xin Liao, Lei Zhang, Jing-Yu Wang, Min-Yan Liao, Qi Qi, Tong Xu, "Security and efficient data dissemination over wireless sensor network with raptor codes", *Machine Learning and Cybernetics (ICMLC) 2013 International Conference on*, vol. 04, pp. 1596-1600, 2013.

[7] Chun Chen , Sammy Chan , Jiajun Bu, "DiCode: DoS-Resistant and Distributed Code Dissemination in Wireless Sensor Networks", IEEE Transactions on Wireless Communications (Volume: 11, Issue: 5, May 2012).

[8] Rui Zhang, Yanchao Zhang, "LR-Seluge: Loss-Resilient and Secure Code Dissemination in Wireless Sensor Networks", *Distributed Computing Systems (ICDCS) 2011 31st International Conference on*, pp. 497-506, 2011, ISSN 1063-6927.

[9] Joshua Ellul, Kirk Martinez, "A Few Bytes are Worth a Thousand Words: Run-Time Compilation of High Level Scripts in Sensor Networks", Distributed Computing Systems Workshops (ICDCSW), 2010 IEEE 30th International

[10] Sukanya C.M] and Sukanya C.M "Integration of Wireless Sensor Networks and Mobile Cloud" (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 6 (1) , 2015, 159-163