ISSN (Online) : 2454 -7190 ISSN (Print) 0973-8975

Copyright © J.Mech.Cont.& Math. Sci., Vol.-14, No.-1, January-February (2019) pp 432-443

A Secure and Efficient Scheduling Mechanism for Emergency Data Transmission in IOT

[1]D. Subba Rao, Dr. [2]N.S. Murti Sarma

[1] Professor, Department of Electronics and Communication Engineering,
Siddhartha Institute of Engineering and Technology, Vinobha Nagar,
Ibrahimpatnam, Hyderabad, Telangana 501506

[2]Professor, Department of Electronics and Communication Engineering,
Sreenidhi Institute of Science & Technology, Ghatkesar, Hyderabad,
Telangana 501506

https://doi.org/10.26782/jmcms.2019.02.00031

Abstract

Internet of things (IOT) enables electronic gadgets to communicate with the server and each other, enabling them to share crucial information. With the advancement in the technology, more and more devices are added to the network of IOT every day. In the era of smart cities, the amount of data being transmitted is immense. While transferring such a huge amount of data, the system has to prioritize the data being sent based on the importance, such as medical and fire safety information. Lack of efficient scheduling algorithms leads to inappropriate delivery of emergency packets, thus rupturing the functionality of the system. Also, the data sent over the network has to guardagainst attacks over the channel. To overcome these drawbacks, a scheduling algorithm named Efficient data emergency aware packet scheduling scheme (EARS), enhanced with data security using Elliptic curve cryptography is proposed in this paper. In EARS, each packet has a description of its priority and the deadline before which it has to reach the sink. This enables easy identification of the emergency nodes. Further, in order to reduce the total number of transmissions in the network, the normal data packets can be network-coded and sent to the destination. This will reduce the congestion in the network. The proposed method is compared with the existing state of the art techniques and the results produced outperformed the exciting methods.

Keywords : network of IOT, efficient scheduling algorithms, Elliptic curve cryptography, emergency nodes, transmissions in the network.

I. Introduction

Internet of Things is the most popularly known creative phenomena of this century. It has gained a lot of popularity with the advancements in the internet technology. IOT based devices are interfaced with multiple sensors and the devices are connected to the cloud to transfer the data [VI].

Figure 1: IOT overview

Internet of things basically expands the interdependence of humans to interact, contribute and collaborate to things around us in figure1. Industrial grade sensors ae embedded into the devices that collect the information form continuously and relay the same to the controller. This data leads to a better understanding of how things work and work together. Internet of things unites the devices with different sensors on to a common platform and thus the devices can communicate with other for better results. The entire process is carried over secure channels to prevent the data from being hacked and corrupted. Once the data reaches the cloud, data analytics is employed to analyze the data and perform control actions [XI].

There are three important concerns while establishing am IOT system.

Connect: For the IOT system to work, one must ensure a proper internet connectivity. All the devices in the network should be connected in order to share the data.

Analyze: The second step is processing of data where the real-time analysis of incoming data streams with event aggregation, filtering and correlation occurs. In this stage, IOT has to identify raw data streams with contextual information and generate composite streams, query and visualize massive amounts of data with integrated cloud service support and enable big data analysis [I].

Integrate: the final step is enterprise connectivity where the critical IOT data and events dispatch dynamically to applications and process flows. API based integration with cloud applications and an IOT device happens in REST APIs. Sending messages to the devices from the enterprise and mobile apps, independent of device connectivity happens in command and control [XIII].

Present day’s IOT for smart cities is most popularly used technology. This IOT technology primarily consists of the wireless and wired sensors integrated with the devices [VII]. The services are also extended to mobile communications, social networks, smart and intelligent transportation etc. Sensors measure the values and send the raw data to the cloud which is analyzed and used for various applications [V]. For the internet of things, there are a series of protocols which are being used, they are CoAP (good for a machine to machine communication but less secured), MQTT, HTTP, XMPP. All these protocols are highly secured [XV]. The hardware used in IOT is open source hardware which consists of microcontrollers. These microcontrollers are small programmable devices and they can be connected very easily.

II. Literature

There are three types of packet scheduling algorithms in IOT, they are as follows

- Deadline-based scheduling
- priority based scheduling
- packet type based scheduling

Deadline-based scheduling:

The type of algorithm used in this scheduling is the RMS algorithm. The data packets are static in nature for the RMS algorithm. In this process, the deadlines for packets are used for packet scheduling [II]. Static priorities are the priorities of packets which are being used in the RMS algorithm. As the priority of the packets is static RMS algorithm is not that much applicable and it will have some limitations.

Priority Based Scheduling:

For overcoming the problems in the deadline scheduling the developers brought priority scheduling into existence [IV]. These priority based scheduling algorithms are again classified into two categories namely: Preemptive scheduling and non-preemptive scheduling. In the non-preemptive scheduling algorithm, the process goes in a specified order. The first started packet which is to be processed will be sent first even if the priority of the second packet is higher than the first. It will allow the second packet only when the processing of the first packet is completed. Preemptive scheduling is somewhat opposite to non-preemptive. Here, the processing of the packet happens according to its priority. If the priority of the packet is higher than its preceding packet, it has to be sent first [IX].

Packet Type Based Scheduling:

The packet type based scheduling scheme is again classified into two categories namely real-time packets and non-real-time packets [III]. In the real-time packet scheduling, real-time packets are prioritized first, with a minimum end-to-end delay. The non real-time packets are very low in their priority and hence these information will be sent with some amount of delay to the base station.The packets priority can be determined by observing the type of the packet which is being used. Chennakesavula proposed a scheduling property, named effective real-time packet scheduling policy (ERTS). In this algorithm, nodes in the dead line of packets utilizes the data andthe order of the packet transmission. Lee proposed a scheduler scheme named as multi-level queue scheduler scheme. Depending on the location of the sensor nodes, queues will be used to send the data [X].

III. Secure EARS - NCECC-EARS

This paper proposes a new secure EARS scheme, Network Coded Elliptic Curve Cryptography (NCECC)-EARS to transfer the data from the source to destination without data tampering representing in figure.2.

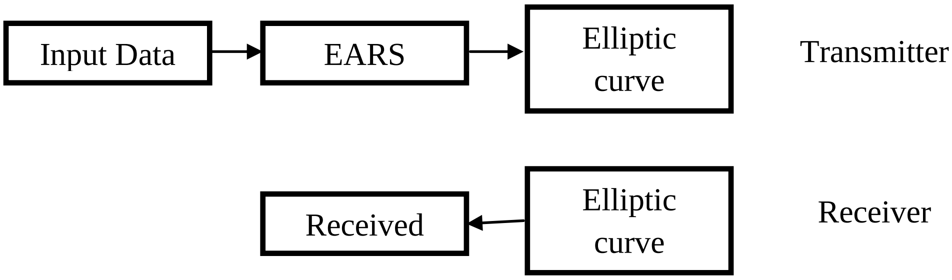


Figure 2: Proposed secure EARS block diagram

In this scheme, the data scheduling is done according to EARS. Once the data packets have been prioritized, the data is encrypted to make the system more robust. The corresponding sections explain the functioning of the algorithms in detail [VIII].

Structure of EARS

EARS techniquehas three modulesnamely

- Access control module (ACM)
- Emergency aware module (EAM)
- Packet forward delta module (PFM).

Figure 3 shows the block diagram of EARS and this consists of 10 nodes which will be starting from a to j.

The function of the node (a) is to give the incoming packet and node (b) takes the received data packet. The function of the node (c) is to take the packet from child nodes which have the highest priority. Nodes (d & h) are for MAC address packet. Node (e) gives the acknowledgeddata packet. Node (f) contains the data with the highest priority. Node (g) is for local priority data packet. Node (I) is for highest priorityinformation packet which uses TDMA to transmit the data. Node (j) is for sending certain results about the MAC address [XIV].

This EARS scheme is mainly designed for applications like emergency fire service. These include applications like rising alarm, positioning information and data retrieved from sensors. In this process, the data packets are basically classified into three categories according to the priority, they are Emergency data packets (pr_1), General data packets (pr_2) and Non-Emergency data packets (pr_3). Before going to learn about the data packets one should learn about the *sink node*.

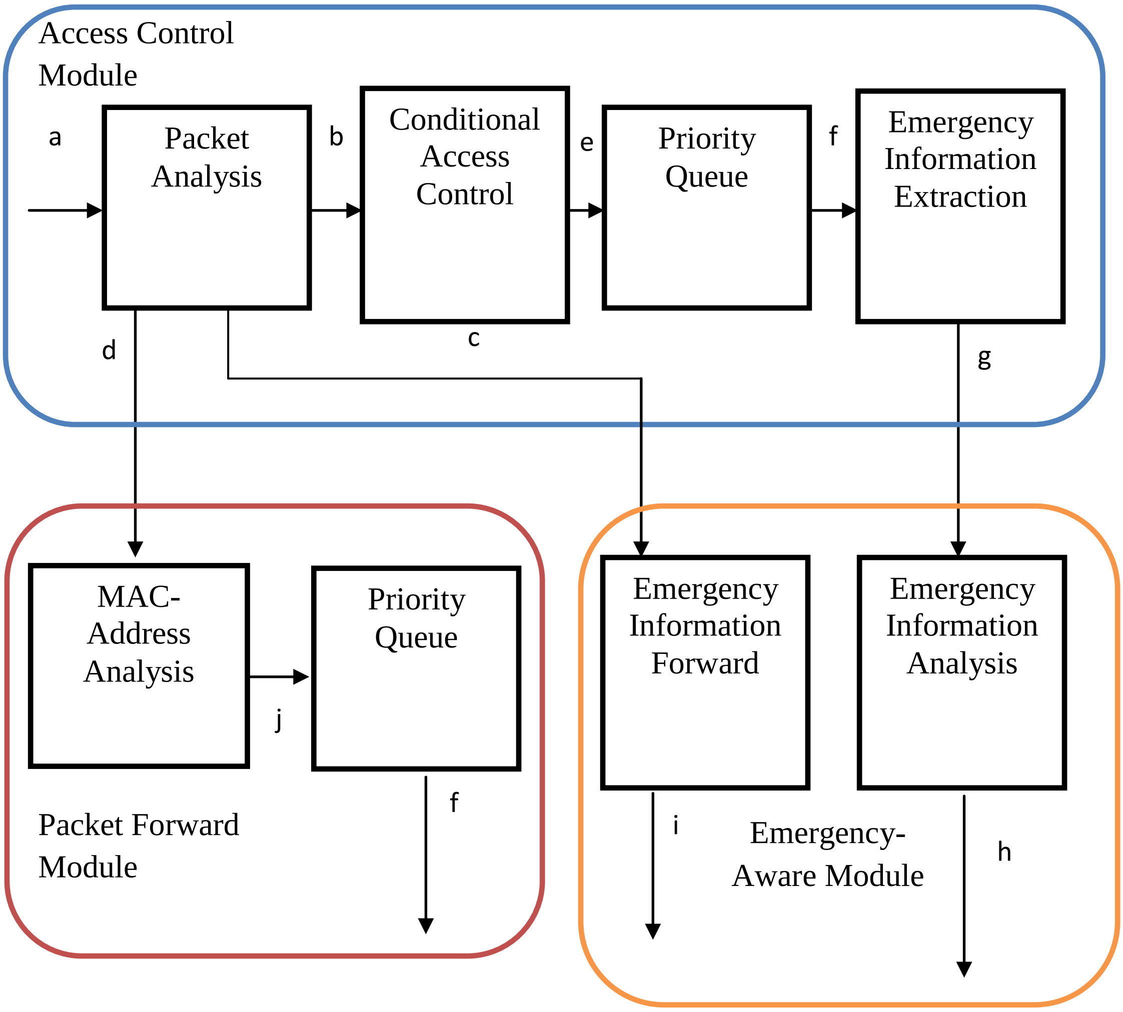


Figure 3: EARS working

Sink node is a place where the data collected by the sensor node in wireless networks is received and stored. The time at which the data packets reach the sink node is given by:

$$D_{e2e} = \sum_{j=1}^{n} (k_j + k_j^l + 2)T$$

Emergency data packets(pr_1): as the name itself suggeststhese packets are of very high priority. The information from these packets should be sent as early as possible to the sink node by ignoring all the low prioritized packets(e.g., the alarm intimation in fire safety applications).

General Data Packets (pr_2): these packets are mostly seen in the online system. This information can be acquired by emergency data packets (e.g., the network information which is present in fire monitoring service).

Non-Emergency Data Packets (pr_3) : these data packets have the least importance when compared to other two types of data packets, so the deadlines of these data packets are longer than the other data packets(e.g., the sensor information of fire monitoring system).

Modules of EARS

Access Control Module:

The purpose of this module is to recognize the receivedinformation packets and process them according to their priority [XIV]. For further processing, the data is fed to the conditional access control (CAC). Here, deadline of the data is checked by the CACand then the packets with highest priority are sent to EAM.MAC address packets are analyzed in packet forward dealt module (PFM). The valid packets are saved in thepriority queues(PQ) [XII].

The three types of priority queues that exist at every node are:

- priority queue A (PQA)
- priority queue B (PQB)
- priority queue C (PQC).

The information packets which have the highest priority like emergency data packets are stored in (PQA). The second highly prioritized packets which are commonly known as general data packets are stored in (PQB). Generally, the lowest prioritized packets are being stored in (PQC). This information is extracted from the emergency nodes and stored in the EAM. The priority and the deadline for the packets are stored as the datapriority information.

Emergency – Aware Module:

EAM mainly deals with the emergency information and the operations that are applied on the data are of Emergency Information Forward (EIF) and Emergency information analysis (EIA). The purpose of the EIF is to send the highest prioritydata packet which is taken from the local nodes and its sibling. This process of data forwarding is terminated when there is no emergency information coming from the sibling nodes. The second phase is to determine where the emergency information packets are gathered from. Then EIA will receive the MAC address packet from the sender node and in the endtransmits the MAC address of the packet to all sibling nodes. Here, if the priority of the packet is high, then the emergency of the packets also will become higher. If the priorities are the same in the information packet then the deadlines for the packets are compared. The packet having the shorter deadline will be considered to have a higher emergency.

Packet Forward Module:

As the name implies, packet forwarding takes place in this module. MAC- address is analyzed when the information or the packet is forwarded from ACM. After the analysis of the MAC address, if the addresses are found to be similar, the cannel is established for the communication to begin. If not, EIF will resend the emergency information packet.

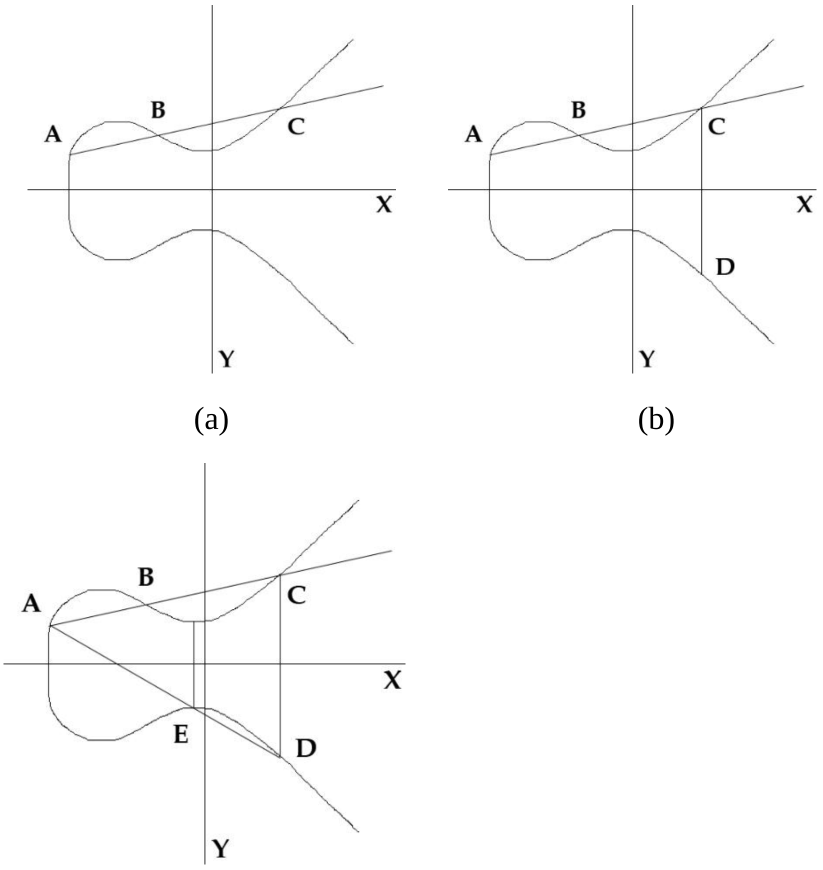
It is mandatory to check the channel flag before the data transfer process starts in the EARS scheme.The channel states are basically classified into three states. Ideal state where no node is using the channel. The second state receives the information from the channel and emergency information packet is sent with Time Division Multiple Access (TDMA)scheme. The MAC address packet is broadcasted by taking the channel and the emergency data packets. In this technique, by controlling the time slot the state of the operation of the channel can be varied. It realizes the packet scheduling and forwarding.

Elliptical Curve Cryptography

Elliptic curve cryptography was invented around the mid-1980s. But no significant work has been implemented in this topic until recent years. This technique is a public key cryptosystem. In public key cryptosystems, the data can be encrypted with the public key, but can only be decrypted with the private key. A concept that is to be discussed in this regard is the trapdoor function. A trapdoor function has a one to one relation between the input and output. But this relation is applicable only in one direction i.e. from input to output. The input cannot be estimated from the output. One such extensively used cryptosystem is RSA. It is based on prime number factorization. The ECC is much faster and efficient system when compared to RSA. This is because, if ECC requires a 256-bit key size to achieve a certain level of security in the data, RSA would require a 3072-bit key. This is one of the reasons that elliptic curve is very popular today.

Consider a graph with X and Y axis as shown in the figure 4a. The elliptic curve is symmetric aboutthe x-axis. The other feature of the graph is that if a straight line is drawn through the curve,it will intersect the curve at no more than three points. Let the points be named A, B and C. now, an interestingphenomenon here is that the dot product of the first two pointsresults in C.

$$A.B = C$$



(a)

(b)

(c)

Figure 4: Stages in Elliptic curve cryptography

A straight line drawn from C on the mirror curve part will also intersect the curve in 3 points. This step is shown in figure 4 c. The process can be extended continuously. Here the dot function can be used "n" number of times, a value obtained from the DOT function can be called as "Z". Assuming that there is a MAX value in X-axis and imagining that the user is applying the dot function in the curve over and over then the values in the curve will look like way out from the X-axis, for overcoming this situation X max is used so that the values crossing from the X max will not be taken into consideration. In the elliptical cryptography system, private key is the number of times the dot function is used in the curve.

IV. Experimental Results

The performance of the system is measured using network delay, energy consumption and throughput. Figure 5 depicts the packet delay time in comparison with the TDMA, EARS and NCECC-EARS scheme.

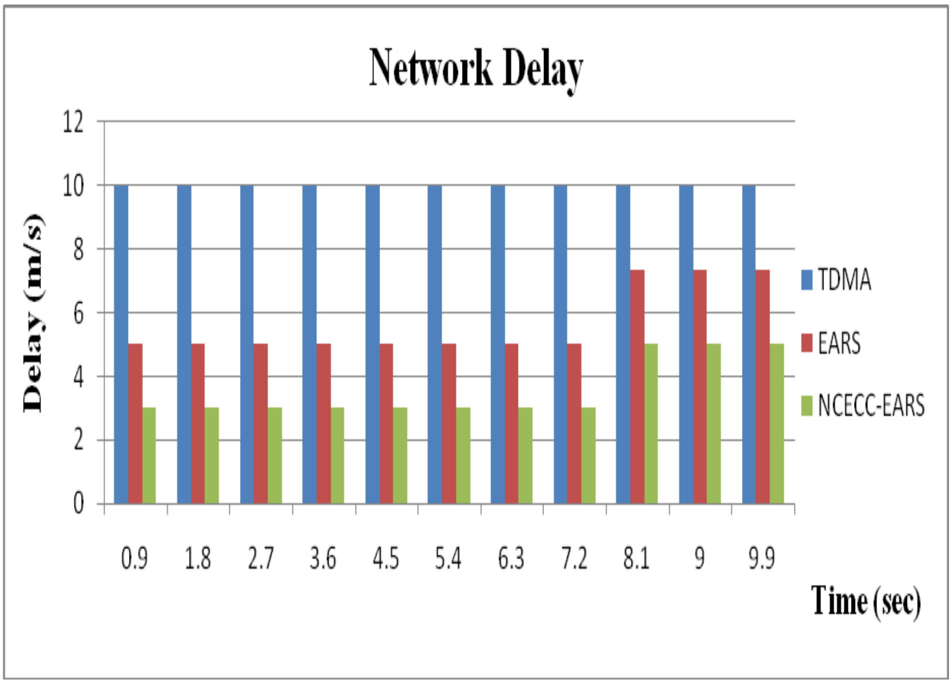


Figure 5:Packet Delay

The packet delay of the proposed technique reduces over time when compared to the existing techniques. The addition of an encryption algorithm leads to secure transmission of the data, thus resulting in reduced delay.

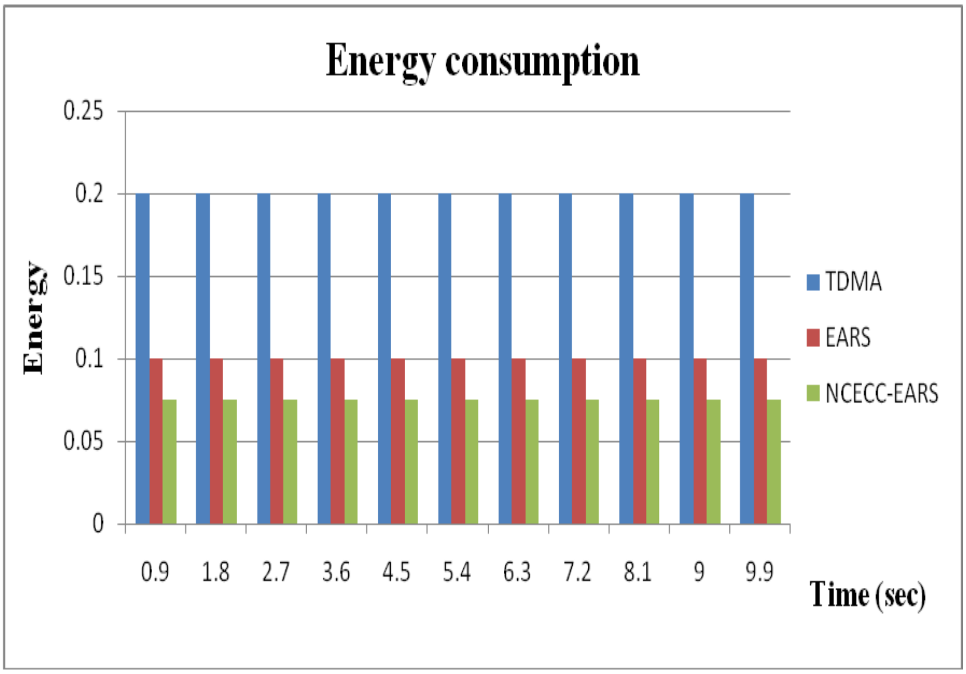


Figure 6: Energy consumption

The energy consumed is the difference in the initial energy and the remaining energy. This energy consumption by the nodes over time reduces. This phenomena is depicted in figure 6.

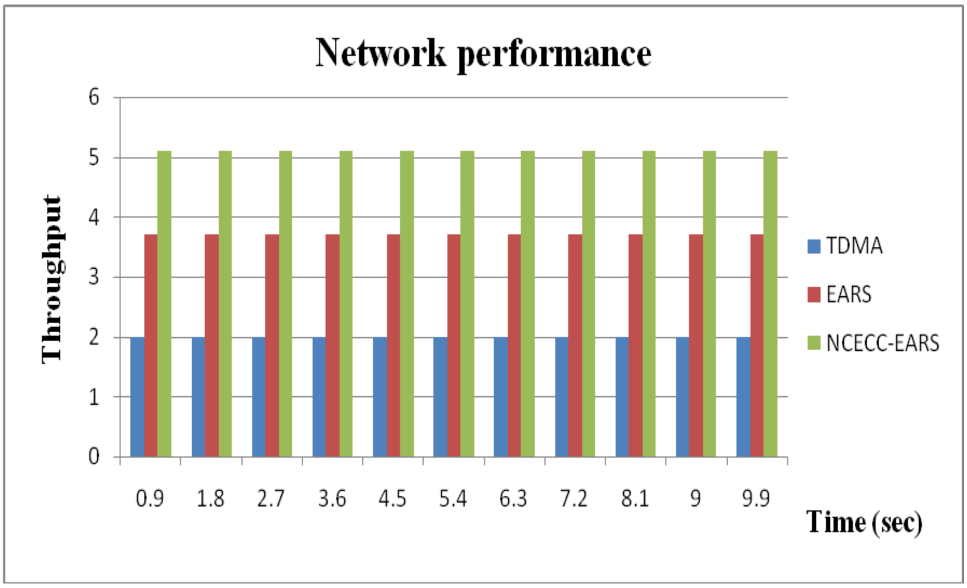


Figure 7: Network Performance

Figure .7 depicts the overall network performance. The throughput of the proposed system exceeds the performance of the EARS and TDMA.

V. Conclusion

The proposed NCECC-EARS scheme is a combination of the conventional EARS scheme and elliptical curve cryptography. In the present day internet revolution, the data integrity is a major challenge. The proposed system thus enhances the data security by encrypting the data before transmission phase, which is then decrypted at the receiver side. The experimental results show that the proposed scheme outperforms the existing counterparts.

References

I. A. T Hashem*et al.*, “The role of big data in smart city,” *Int. J. Inf. Manage.*, vol. 36, no. 5, pp. 748–758, 2016.

II. F. Yang and I. Aug´e-Blum, “Delivery ratio-maximized wakeup scheduling for ultra-low duty-cycled WSN under real-time constraints,” *Comput.Netw.*, vol. 55, no. 3, pp. 497–513, 2011.

III. G. Lu and B. Krishnamachari, “Minimum latency joint scheduling and routing in wireless sensor networks,” *Ad Hoc Netw.*, vol. 5, no. 6, pp. 832–843, 2007.

IV. K.-H. Phung, B. Lemmens,M. Goossens, A. Nowe, L. Tran, and K. Steenhaut, “Schedule-based multi-channel communication in wireless sensor networks: A complete design and performance evaluation,” *Ad Hoc Netw.*, vol. 26, pp. 88–102, 2015.

V. M. Nitti, R. Girau, and L. Atzori, “Trustworthiness management in the social internet of things,” *IEEE Trans. Knowl. Data Eng.*, vol. 26, no. 5, pp. 1253–1266, May 2014.

VI. M. V. Moreno *et al.*, “Applicability of big data techniques to smart cities deployments,” *IEEE Trans. Ind. Informat.*, vol. 13, no. 2, pp. 800–809, Apr. 2017.

VII. P. Guo, T. Jiang, Q. Zhang, and K. Zhang, “Sleep scheduling for critical event monitoring in wireless sensor networks,” *IEEE Trans. ParallelDistrib. Syst.*, vol. 23, no. 2, pp. 345–352, Feb. 2012.

VIII. R. Gomathi and N. Mahendran, "An efficient data packet scheduling schemes in wireless sensor networks," in *Proc. Int. Conf. Electron. Commun.Syst.*, Feb. 26–27, 2015, pp. 542–547.

IX. T.Qiu,K. Zheng, H. Song, M. Han, and B.Kantarci, "A local-optimization emergency scheduling scheme with self-recovery for smart grid," *IEEETrans. Ind. Inf*, doi: 10.1109/TII.2017.2715844.

X. T. Qiu, R. Qiao, and D. Wu, "EABS: An event-aware backpressure scheduling scheme for emergency internet of things," *IEEE Trans. MobileComput.*, doi: 10.1109/TMC.2017.2702670.

XI. U. Jang, S. Lee, and S. Yoo, "Optimal wake-up scheduling of data gathering trees for wireless sensor networks," *J. Parallel Distrib. Comput.*, vol. 72, no. 4, pp. 536–546, 2012.

XII. V. Chang, "Towards a big data system disaster recovery in a private cloud," *Ad Hoc Netw.*, vol. 35, pp. 65–82, 2015.

XIII. X. Shen, C. Bo, J. Zhang, S. Tang, X. Mao, and G. Dai, "EFCon: Energy flow control for sustainable wireless sensor networks," *Ad Hoc Netw.*, vol. 11, no. 4, pp. 1421–1431, 2013.

XIV. Xue, B. Ramamurthy, and M. C. Vuran, "SDRCS: A servicedifferentiated real-time communication scheme for event sensing in wireless sensor networks," *Comput. Netw.*, vol. 55, no. 15, pp. 3287–3302, 2011.

XV. X. Xu, X. Li, andM. Song, "Distributed scheduling for real-time data collection in wireless sensor networks," in *Proc. IEEE Global Telecommun.Conf.*, Dec. 9–13, 2013, pp. 426–431.