Dynamic Traingular Localization Based Security Aware Protocol Forwireless Sensor Networks

Navneet Kaur, Supreet Kaur

Abstract: development of the internet technologies provides directed towards emergence associated with Wireless sensor networks. This is because of his / her highly effective characteristics in comparison with his or her counterparts associated with related ways such as barcodes. Throughout recent times, RFID generally based mostly solutions tend to be the only many extensively multiply products with regards to paying attention to though monitoring functions having WSN deployment. One of many knowledgeable deployments having WSN is usually through radio-frequency personality (RFID) technology. Compared, radio-frequency detection solutions are afflicted with many assaults and basic safety provocations. In this paper, a novel dynamic triangular localization based security protocol for wireless sensor networks. Elliptic curve cryptography model is also used to enhance the results further. Extensive experiments reveal that the proposed technique outperforms the existing techniques.

Keyword: WSN, clarifications, types security challenges, Security and awareness, Secure Routing ECC.

1. INTRODUCTION:

WSN is composed of large number of tiny nodes with no infrastructure. All the nodes will collect the information and transmit it to another node. The architecture of the wireless sensor network .It consists of four major parts namely. WSN spatially scattered independent devices using sensors to observe physical and environmental conditions. It is initiated with the basic features of wireless sensor networks and issues taking place in practical applications. Motivation towards the present investigation leads to advance features in (WSN). The problem defined in this work was illustrated to achieve the objective of the research work. Finally the chapter describes the proposed contribution in the current work and defines the output of this work. Most people are likely to be consistently creating modern advances that allow humanity to wide spread their needs. WSNs quite region yet, buying executive composing of multifunction alarm system nodes which have been modestly more prominent plus converse wirelessly all around reasonably limited distances. The initial elements linked to WSNs give a boost to adaptability decreasing unique donation inside usable jobs for example battlefields. WSNs can easily perform a vital role in maximum applications, which includes patient healthiness, checking the environmental remark in addition to also be developing building infiltration surveillance. In due course WSNs are generally a significant part in the lives. The introduction of wireless sensor sites was actually encouraged by armed service applications i.e. battlefield security. But, wireless sensor network is actually found in various civilian request areas, involving.

1.1WIRELESS SENSOR NETWORKS

WSNs are dynamic and that can contain various styles of sensor hubs. The sensor hub structure works with minimal effort, increment adaptability and furthermore offers the adaptation to non-critical failure. It likewise considers the advancement procedure and monitoring vitality. The system of sensor hub contains detecting unit, preparing unit, correspondence unit and power source unit. The fundamental squares for a sensor hub can be appeared in Compact clarifications of sorts are as these:

1.1.1 Sensing Unit

It involves a determination of disparate sorts of sensor which is required for measurement of the event with the physical condition. Identifiers are chosen predicated on their application. The sensor's result is typically an electric flag which happens to be for the most part simple.

1.1.2 Processing Unit

It requests a processor chip (microcontroller) and storage room (RAM). Besides, they have frameworks and a clock. The obligation from the control gadget incorporates gathering information from different assets at that point taking care of and putting away. A clock is used to achieve the sequencing to the systems.

1.1.3 Communication Unit

It operates on the transceiver that contains a transmitter plus a receiver. Communication is completed with the communication stations utilizing network protocols. Predicated about the form requirements and relevance to be able to create a good communication it normally operates on an excellent method, for instance, radio, infrared or optical communication.

1.1.4 Power Device

Every work connected with the capability device would be to give the power to the sensing unit node to get monitoring the environment at an affordable and fewer times. The relationship of the sending unit is determined by the electrical power and also a potential electrical generator which happens to be connected to the strength unit. As Power device is critical for the skilled technique power.

1.2 Types of WSN

1.2.1 Terrestrial WSN:

Consists of thousands of nodes and it is placed randomly in the network area. Here communication via base station is very easy. Due to wastage of power, external sources like

- *Computer science and engineering department*
- *Khalsa college of engineering and technology*
- *Amritsar*
- *Navneetsappal2@gmail.com*
- *Computer science and engineering department*
- *Khalsa college of engineering and technology*
- *amritsar*
- *oberoisupreet9@gmail.com*

solar cells are used. Energy can be conserved with minimum transmitter range, reducing delay, multi hop routing.

1.2.2. Underground WSN

Consists of more number of sensors which are placed underground or in caves used to monitor soil and rocks Condition. Even some nodes are placed above ground surface for communication to the base station. The most important drawback in this type of difficult to replace the underground nodes when battery power is low.

1.2.3 Underwater WSN

Consist of number of sensor nodes and vehicles deployed under water. Autonomous vehicle is used for collecting in order from sensor nodes. Underwater communication can be done by acoustic waves. These nodes are self con figure able and cannot be replaced when battery is low.

.

1.3 SECURITY CHALLENGES IN WSN

This valuable an individual section which unfortunately instance, in brief on the subject of the issue found in WSNs mainly as data privacy, consistency, veracity, key establishment, privacy, protected redirecting, secure group management, authentication intrusion recognition, availability and also protected details aggregation.

1.3.1 Data Confidentiality

In order to get computer data from the eavesdropper, one must end up being promise obtaining the confidentiality involving sensed data. To achieve the information confidentially, the encrypted shield feature is usually needed.

- An important WSN didn't break free of sensing unit browsing to help us, neighbors. Because in some uses, computer data saved within a sensing unit node may very well be exceptionally delicate. Consequently to counteract leakage involving the fragile computer data some sort of sensing unit node should, so, avoid writing first considerations used by the encrypted shield and additionally decryption of nearby nodes.
- This gets station will be contained in WSN's.
- Community is sensing unit material as an example, just as sensors ‘identities likewise ought to be secured a little to help us preserve next to potential customers' analysis attacks.

1.3.2 Data Integrity

Records strength or data integrity situations in wireless networks are precisely like those in restless networks. Records strength makes certain of which virtually any gotten details is simply not happened to be erased and also metabolized in transit. One has gotten note, a resister may unveil modifying strikes the moment cryptographic checking out mechanisms, for example information authentication principles and even hashes usually aren't used. Case in point, harmful node will then start being active. Broken phrases and also vary the data in a packet. That brand new small fortune could very well be therefore brought to you for the person who is original.

1.3.3 Authentication

Authentication can be a task which often helps some node to be able to read the origins of one's packet boat and even guarantee the dependability associated with the data. For WSNs the device is simply not some simply limited to switching info the packets. It would likely improve your entire packet boat watch just by treating additional packets. The actual receiver node, accordingly, has to be sure that the information utilized in a decision-making procedure sounds from precious resources. For an abundance of programs, authentication can be upon essential as a consequence of issues with sensitivity.

1.3.4 Secure Routing

The most important activity is defined to ensure that every advanced node is unable to eliminate current nodes or simply create extra nodes in the linked path. On the other hand, in real life, a fabulous safe, secure routing or course-plotting process assurances all the stability, genuineness, together with the availability of messages inside an adversary. Risk-free course-plotting methodologies meant for supplying security by a resource that will getaway inside WSN's need to meet the future requirements:

a) Remoteness within the unwanted nodes via method finding protocols.
b) This networking topology which in turn is dependent upon all the tough networking bonds ought not to be launched from an adversary.
c) Reliability connected with walkways will have to be preserved. Routinely, an attacker could misdirect all the networking by way of marketing and advertising counterfeit smallest pathway and possibly bringing about offering connected with loops.
d) Mail messages adjusting by way of an adversary together with aberrant all the nodes are generally recognized.
e) Unauthorized or simply aberrant nodes ought not to be capable of switch course-plotting communications.

1.3.5 Intrusion Detection

Intrusion detection is a kind of security organization strategy intended for a person's laptop and even networks. An Intrusion detection strategy (IDS) accumulates and even assesses information and facts out of unique areas during isn't even close to or even system to identify achievable security breaches, for example, each intrusion (attacks externally any organization) and even maltreatment (attacks from the inside any organization). Breach detection functions incorporate the foregoing:

a) Observation and even homework of each prospect and even strategy activities.
b) Look at the device layouts and even vulnerabilities.
c) Review of strategy and even archive integrity.
d) Potential to obtain prevalent structures of attacks.
e) Analysis of the odd recreation patterns.
f) Tracking of the people coverage violations.

1.4 Security and energy awareness

Security as well as awareness in cluster head when deciding on cluster heads, here be various techniques to save lots of energy.

1.4.1 Network Model WSNs include various node. All these nodes can certainly be able of indication the actual sensed or discovered facts so that you can the camp section or destroy node. This sign pattern of each and every destroy node can be based on the consistent supply, the place the idea markets the info by using utmost radio station variety in the range. This specific collection of sensor / probe nodes kinds the chaos, which can be embodied like a network. Inside every chaos, the expression shows the related chaos head. Together, this method to propagate

1.4.1 Energy awareness:
the cluster head collection mold use the hybrid protocol with party explore optimization (GSO) plus Greyish Hair optimization (GWO), simply by thinking about the factors including distance, wait, vitality, and the risk factor. In truth, wait, the space relating to the based mostly nodes plus group heads. The danger truth or perhaps need to be debilitated for your useful group head assortment unit, whereas the vitality with the group head will have to keep on being high. Hence, based on these demands, provides the purpose minimization functionality for your group head selection.

1.4.2 Security awareness:
This fragment illustrate the cluster head part mold bas ed inside security constraint. at the same time as relating to the security limitation, the particular 3 ways regarding Security awareness involve Security awareness manner, dangerous manner as well as γ-risky manner are to be considered. Your criteria regarding the 3 ways is usually depicted inside the next subsections.

1.4.3 Security mode:
Security awareness manner: Your security mode operation selects the group go of which satisfies the need for security. Below, as well as Security mode means Security awareness demand from customers as well as Security awareness status associated with the group go choice, respectively. If the node attains the matter SD≤SR, it usually is certified for the reason that desired set head. What's more, is your conventional tactic which is often deemed a good mode Dangerous manner: This kind of manner decides the active group go to let the suitable group go choice, as well as a result it can take the entire possible risks. Subsequently, the dangerous manner is regarded as the extreme manner while in the group go choice process. Y-risky manner: The cluster head that can hold at nearly all γ-risk tend to be selected during the selection process determined by γ-risky function. Below, γ is definitely the odds calculate using two opposites γ= 0 as well as γ= 1 (i.e. 100%) comparable to the dangerous as well as Security awareness mode.

2. LITERATURE SURVEY

N. M. SARAVANA Kumar et al. (2015) [1] encouraged the unique, proven discovery strategy pertaining to unveiling direction-finding problems. For almost any regarded injury, it gives you given exclusive, in relation to that will the rules are intended because of the guiding foundation occurring for being experimented with pertaining to unveiling many directions-finding indicates pertaining to representation wormhole, dark colored beginning, plus Sybil episode. This simulated positive aspects show that will procedure escalates the particular robustness involving specifics by way of (measuring) celebrating the important things such as package shipping amount plus throughput although unveiling the important direction-finding attacks. JAYASEELANJ et al. (2013) [2] discussed a cluster based plan that augments High Energy First (HEF) clustering algorithm and enables multi-hop transmissions among the cluster by fusing the choice of sending and getting nodes. Proposed system's performance is evaluated based on energy efficiency and reliability. As compared to LEACH, it enhances the lifetime of network of nodes remain a-lived. HEF algorithms proves that use of fuzzy variables i.e. concentration, energy and density, enhances network lifetime to great extent. Giving dependable framework conduct an ensured hard network lifetime is a testing undertaking to well being basic and exceedingly solid WSN applications. Liu et al. (2014) [3] discussed a novel deployment algorithm called ACO-greedy algorithm which combines the basic ACO with greedy migration mechanism, to solve the problem of grid-based coverage with low-cost and connectivity-guarantee (GCLC). In-spite of this advantage the ACO-Greedy can dynamically changes the detecting/correspondence radius to decrease consumption of energy, thus enhances lifetime of network. Results demonstrate that proposed methodology decreases the deployment cost, enhances energy efficiency and lifetime of network in grid based WSNs. GHOTRAet al. (2015) [4] Proposed ACO based RZ LEACH with mobile sink algorithm, which utilizes inter-cluster ACO alongside RZ nodes for transmitting data in WSN. Addition of ACO helps From the above literature survey, it is noted that with the rapid development in system interactive media types of gear has permitted extra constant advanced administrations for example video-conferencing, web recreations to grow to be the conventional internet tasks. The multicast portrays the appropriation of structures from only one single hub to number of destinations. These constant administrations have a rigorous need of QOS elements like data transfer capacity, delay, and jitter and so forth to guarantee perfect, steady, and reasonable sign to the collectors. WSNs have gotten to be significant region of exploration in computational hypothesis because of its extensive variety of uses. Be that as it may, because of constrained battery control the vitality utilization has gotten to be significant constraints of WSNs conventions. In spite of the fact that numerous conventions has been researched so far to enhance the vitality effectiveness advance yet at the same time much improvement should be possible. Tree based routing protocol has demonstrated very huge results over the accessible sensor network conventions. MOTTAGHI et al. (2015) [5] proposed RZ LEACH with mobile sink algorithm. This approach combines the concept of LEACH protocol, Mobile Sink (MS) and rendezvous point (RP) for enhancing results. Concept of moving sink i.e. MS helps in reducing the transmission distance while RN acts as store point means it will transmit only when MS comes closer to it. The result demonstrates that proposed technique works well especially for large area of networks. M Patel, A Aggarwal (2019) [6] Remote sensor systems are defenseless against a lot more assaults. Wormhole assault

is risky to remote sensor systems since it is an entryway to a lot more assaults, for example, dark gaps, dim gap, Sybil, jellyfish, disavowal of administration. Without realizing the conventions utilized in the system, an aggressor dispatches a wormhole assault by setting two vindictive hubs in two distinct pieces of the system which are far from one another. Along these lines, an assailant attempts to irritate the directing procedure. V. Sujatha et al. (2015) [7] Suggested a light-weight structure in this report to help recognize the revolutionary particular information regarding Sybil nodes, but doesn't work with direct, reliable 3rd party, the idea utilizes town RSS to help distinguish relating to the reliability along with Sybil identities. RSS based mostly method is required by this report to help recognize Sybil episodes around a radio alarm network. In line with copy writers, it can be tested a discovery building up a tolerance can be utilized to make variance involving reliable completely new nodes along with completely new vicious identities. Throughput, bundle great loss rate, accurate optimistic charges, end-to-end waits, untrue optimistic charges are widely used to assess the actual functionality of the system. In line with copy writers, the actual simulator benefits demonstrate that building has got if you are a regarding accuracy and reliability by using discovery method offers us our prime accurate optimistic charges nearly 80% by using small untrue optimistic charges in which array to help 16%. Marian et al. (2015) [8] presented a sturdy and light-weight option which usually is essential regarding Sybil strike form detectors, predicated upon RSSI (received indicate toughness indicator). In today current WSN warning systems, there are 2 regarded alerts regarding website link superior evaluation [28]. Obtained Indicate Toughness Gauge and also URL Good quality Gauge (LQI). Creators verified via studies that will RSSI has been constant adequate any time obtained in interference setting sufficient reason for very good transceivers. In accordance with wi-fi direct versions, obtained electrical power should be thought about your purpose of length, nevertheless creators tried on the extender to help localize Sybil nodes. GAOLIUA ZHENG Yan (2018) [9] Portable Ad Hoc Network (MANET) is getting to be one sort of major cutting edge remote systems. By the by, it effectively experiences different assaults because of its particular qualities. So as to assess and gauge the security of MANET continuously and influence this system to respond as needs be, a promising option is to.

4. GAPS IN LITERATURE:

1. The speed of data encryption is still an challenging issue.
2. The use of Cellular automata is ignored by the most of the existing researchers in the field of WSN.
3. The use of ECC in Cellular automata techniques is still an open area of research.

4.1 PROPOSEDALGORITHM

4.1.1Elliptic-curve cryptography (ECC):

Having it's relatively little key measurement (ECC) elliptic-curve cryptography is recognized as your public-key cryptographic protocol of choice alarm networks sensor network .Throughout ECC, an email for being password-protected, or maybe in an electronic signed, can be displayed because some any finite arena, and cryptographic businesses within this message are usually recognized via a string regarding finite arena arithmetic operations. A utilized finite arena portrayal has a bearing on your functionality of your ECC performance. Throughout this exertion, we all implement ECC over GF (p^m) applying the perfect off shoot arena portrayal .The finite arena .GF (p^m)is considered secure and utilizing to get using ECC whether it's adequately huge, as well as its area file format level Michael is actually best [10]. Around implementations of ECC above GF (p^m), numerous specific area arithmetic procedures, just like accessory, subtraction, multiplication as well as inversion, are carried out inside GF (p^m) Inversion, this slowest arithmetic functioning inside ECC, is usually definitely avoided by utilizing projective coordinates. Consequently, in case we do not depend inversion, multiplication remains to be the almost all costly arithmetic functioning and any speedup inside multiplication would certainly immediately create a speedup in ECC implementation.

EDWARD shapes are generally a fresh method of elliptic shapes planned to get ECC. Throughout this work, all of us applied the particular Edwards contour defined by the particular equation $(x^2 + y^2 = c^2 (1 + dx^2y^2)$ The actual elliptic-curve position sum $p_1(x_3, y^3)$ of the two distinctpoints $p_1(x_1, y_1)$ and $p_2(x_2, y_2)$ P2(x2, y2) on this Edwards curve can be found as:

$$x_3 = \frac{x_1 y_1 + y_1 y_2}{c(1+dx_1 x_3 y_1 y_2)} \; y_3 = \frac{y_1 y_1 + x_1 x_2}{c(1+dx_1 x_3 y_1 y_2)} \ldots\ldots\ldots (1)$$

As well as elliptic-curve point bottle $P_2(x_1, y_1)$ of the point $P_2(x_2, y_2)$ can be located as:

$$x_2 = \frac{2x1y1^c}{x_1^2 + y_1^2} \quad y_2 = \frac{(y_1^2 + y_1^2)c}{2c^2(x_1^2 + y_{1)}^2} \ldots\ldots\ldots (2)$$

With the work, most people utilized the particular Edwards curve with random, and 1, over$x^2 + y^2 = c^2(1 + dx^2y^2)$ with $c = 1, d$ arbitrary, and $dc^4 \neq 1$ 1, more than the particular perfect area GF$((2^{13} - 1))^{13}$ Most of us applied the particular Edwards contour projective position improvement and also doubling formulae offered by using Algorithms 3 and also 4 , where 8 and also 5 short-lived parameters are widely-used, in that order. The actual point-at-infinity in this set up can be A pleasant benefit with Edwards contour position businesses is that often virtually no additional be concerned is needed to tackle businesses while using the point-at-infinity.

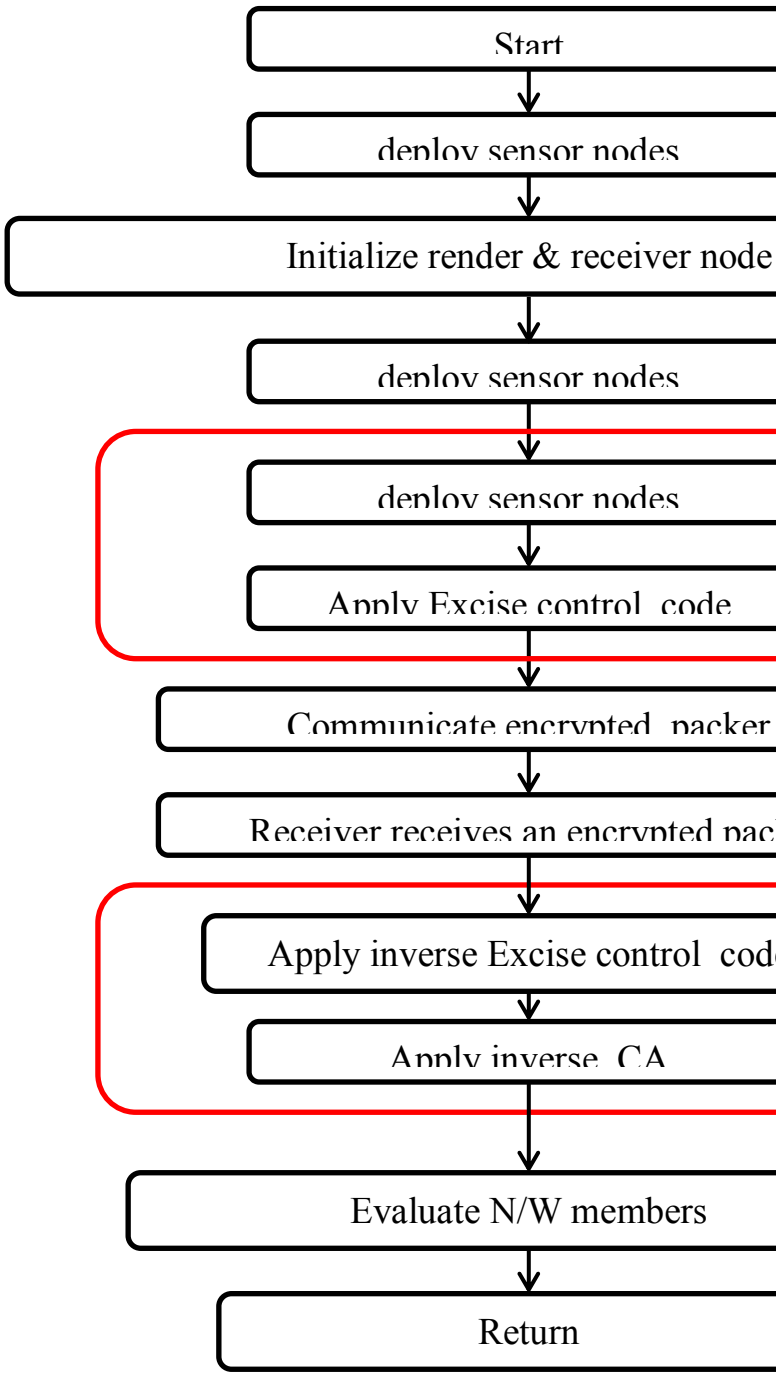
Algorithm 3 Elliptic-curve level improvement method within projective coordinates with regard to Edwards curves.

Involve: $P_1\ (x_1,\ y_1,\ z_1)$ and $P_2\ (x_2,\ y_2,\ z_2)$
Ensure: $P_3\ (x_3,\ y_3,\ z_3) = P_1 + P_2$

1. $T_1 \leftarrow x_1, T_2 \leftarrow y1\, y_1, T_3 \leftarrow z1, T_4 \leftarrow x2, T_5 \leftarrow y^2, T_6 \leftarrow z_2$
2. $T_3 \leftarrow T_3 T_6$
3: $T_7 \leftarrow T_1 T_2$
4: $T_8 \leftarrow T_4 T_5$
5: $T_1 \leftarrow T_1 T_4$
6: $T_2 \leftarrow T_2 T_5$
7: $T_7 \leftarrow T_7 T_8$

8: $T_7 \leftarrow T_7 T_1$
9: $T_7 \leftarrow T_7 T_2$
10: $T_7 \leftarrow T_7 T_3$
11: $T_8 \leftarrow T_1 T_2$
12:$T_8 \leftarrow d \,.\, T_8$
13: $T_2 T_2 \leftarrow T_1$
14: $T_2 T_2 \leftarrow T_3$
15: $T_3 \leftarrow T_3$
16: $T_1 : \leftarrow T_3 - T_8$
17: $T_3 \leftarrow T_3 + T_8$
18: $T_2 \leftarrow T_2 . T_3$
19: $T_3 \leftarrow T_3 . T_1$
20: $T_1 \leftarrow T_1 . T_7$
21: $x^3\ T_1, y_3 \leftarrow T_2, z_3 \leftarrow T_3$

Most of us implemented the actual ECC scalar factor multiplication function, for random and glued points, on Texas Instrument's low-power 1-series 16- little bit microcontroller. Most of us used the actual IAR Included Workbench while each of our progress ecosystem and bought correct time pattern counts.



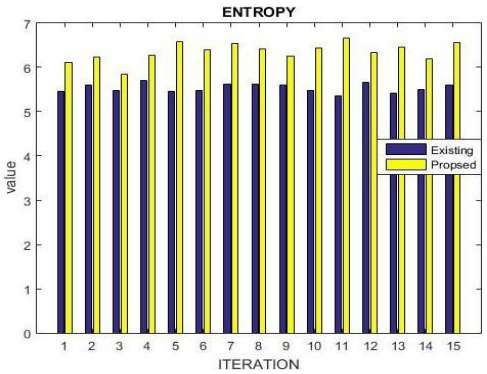
4.1 RESULTS AND DISCUSSIONS

The proposed algorithm is tested on various stages. The algorithm is applied using various performance indices like Entropy, Half Node Dead, Network Lifetime and throughput. ENTROPY: Table 1 is displaying this quantized analysis of the stable period. They have definitely proven how the stable period is highest with the proposed algorithm therefore algorithm is providing better results than the available methods.

TABLE 1: *ENTROPY*

ITERATION	EXISTING	PROPOSED
1	5.4509	6.1179
2	5.5919	6.2259
3	5.4701	5.8431

4	5.7008	6.2835
5	5.4515	6.5851
6	5.4752	6.4037
7	5.6312	6.5462
8	5.6272	6.4243
9	5.6061	6.2650
10	5.4821	6.4480
11	5.3618	6.6591
12	5.6648	6.3364
13	5.4155	6.4541
14	5.5078	6.1900
15	5.6021	6.5524

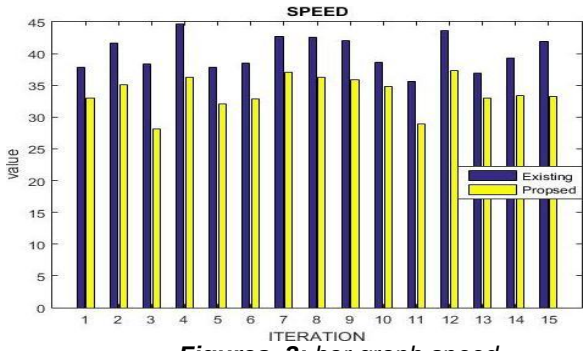


Figures .1: *bar graph Entropy*

As shown in below given figures, we are comparing the results. As results show that our proposed approach results are much better than existing approach. SPEED: Table 2 is displaying this quantized analysis of the speed. They have definitely proven how the speed is highest with the proposed algorithm therefore algorithm is providing better results than the available methods.

TABLE 2: *SPEED*

ITERATION	EXISTING	PROPOSED
1	37.8620	32.9812
2	41.5944	35.0813
3	38.3499	28.1884
4	44.7250	36.2542
5	37.8764	32.0733
6	38.4787	32.8315
7	42.6973	37.1273
8	42.5832	36.2912
9	41.9883	35.8734
10	38.6562	34.8274
11	35.6780	28.9334
12	43.6646	37.3676
13	36.9776	32.9670
14	39.3241	33.3688
15	41.8757	33.2775



Figures .2: *bar graph speed*

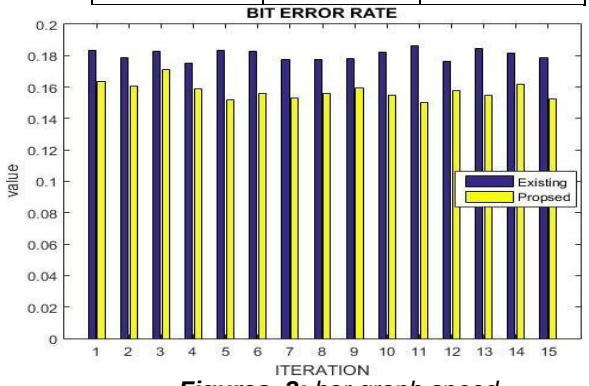
As shown in below given figures, we are comparing the results. As results show that our proposed approach results are much better than existing approach.

3. BIT ERROR RATE:

Table 3 is displaying this quantized analysis of the bit error rate. They have definitely proven how the bit error rate is highest with the proposed algorithm therefore algorithm is providing better results than the available methods.

TABLE 3: *BIT ERROR RATE*

ITERATION	EXISTING	PROPOSED
1	0.1835	0.1635
2	0.1788	0.1606
3	0.1828	0.1711
4	0.1754	0.1591
5	0.1834	0.1519
6	0.1826	0.1562
7	0.1776	0.1528
8	0.1777	0.1557
9	0.1784	0.1596
10	0.1824	0.1551
11	0.1865	0.1502
12	0.1765	0.1578
13	0.1847	0.1549
14	0.1816	0.1616
15	0.1785	0.1526



Figures .3: *bar graph speed*

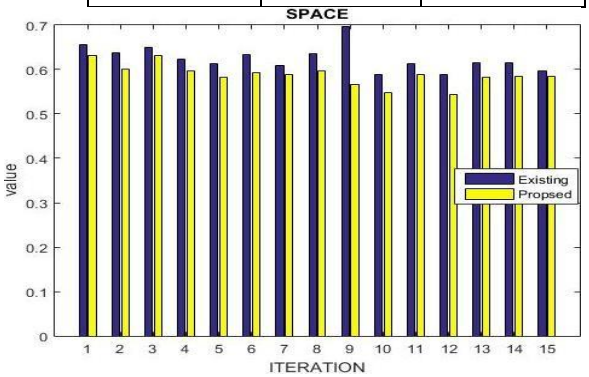
As shown in below given figures, we are comparing the results. As results show that our proposed approach results are much better than existing approach.

4. SPACE

Table 4 is displaying this quantized analysis of the space. They have definitely proven how the space is highest with the proposed algorithm therefore algorithm is providing better results than the available methods.

TABLE 4: *SPACE*

ITERATION	EXISTING	PROPOSED
1	0.6556	0.6313
2	0.6375	0.6011
3	0.6500	0.6309
4	0.6233	0.5962
5	0.6134	0.5822
6	0.6334	0.5933
7	0.6100	0.5880
8	0.6356	0.5960
9	0.6969	0.5672
10	0.5879	0.5480
11	0.6125	0.5880
12	0.5881	0.5435
13	0.6163	0.5835
14	0.6144	0.5846
15	0.5961	0.5854



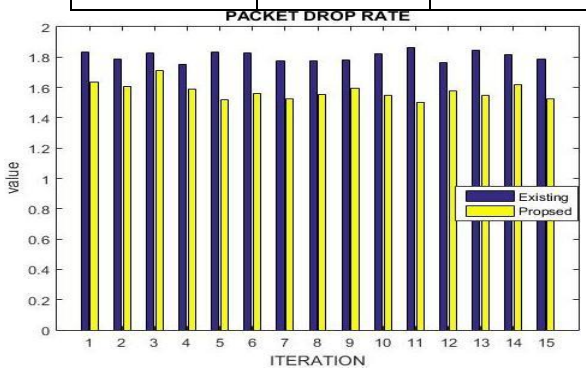
Figures .4: *bar graph speed*

As shown in below given figures, we are comparing the results. As results show that our proposed approach results are much better than existing approach.\

5. PACKET DROP RATE: Table 5 is displaying this quantized analysis of the packet drop rate. They have definitely proven how the packet drop rate is highest with the proposed algorithm therefore algorithm is providing better results than the available methods.

TABLE 5: *PACKET DROP RATE*

ITERATION	EXISTING	PROPOSED
1	1.8346	1.6346
2	1.7883	1.6062
3	1.8281	1.7114
4	1.7541	1.5915
5	1.8344	1.5186
6	1.8264	1.5616
7	1.7758	1.5276
8	1.7771	1.5566
9	1.7838	1.5962
10	1.8241	1.5509
11	1.8650	1.5017
12	1.7653	1.5782
13	1.8466	1.5494
14	1.8156	1.6155
15	1.7851	1.5261



Figures .5: *bar graph speed*

As shown in below given figures, we are comparing the results. As results show that our proposed approach results are much better than existing approach.

CONCLUSTION

In recent times, RFID based systems are one of the most widely spread applications for tagging and keep tracking purposes in WSN deployment. This is due to their powerful features compared to their counterparts of similar techniques such as barcodes. In contrast, radio-frequency identification systems suffer from various attacks and security threats. The wireless channel used for communication is responsible for the majority of these vulnerabilities.In this paepr, a new radio-frequency identification authentication protocol based on Elliptic curve cryptography (ECC) has been proposed. The proposed technique overcomes the issue of RFID vulnerabilities against various network attacks. The proposed technique has improved the performance of ECC based wireless sensor network security protocols using Cellular automata. Therefore it provides results at good computational speed.

REFERENCES

[1] Sarigiannidis, P., Karapistoli, E., & Economides, A. A. (2015). Detecting Sybil attacks in wireless sensor networks using UWB ranging-based information. Expert Systems with Applications, 42(21), 7560-7572.

[2] Jayaseelan, G. and Rajalakshmi, S.K. (2013), “Hard network lifetime wireless sensor networks with high energy first clustering”, International Journal of Engineering Science and Technology, 5(3), pp.618.

[3] Liu, X. and He, D. (2014),“Ant colony optimization with greedy migration mechanism for node deployment in wireless sensor networks”, Journal of Network and Computer Applications, 39, pp.310-318.

[4] Ghotra, A. and Soni, N. (2015), “Performance Evaluation of Ant ColonyOptimizationBased

Rendezvous Leach UsingForMobileSink BasedWSNs", International Journal of Engineering Research and Development, 07 (July 2015), pp.43-49.

[5] Mottaghi, S. and Zahabi, M.R. (2015), "Optimizing LEACH clustering algorithm with sink and rendezvous nodes", AEU-International Journal of Electronics and Communications, 69(2), pp.507-514.

[6] Patel, M., Aggarwal, A., &Chaubey, N. (2019). Detection of Wormhole Attack in Static Wireless Sensor Networks. In Advances in Computer Communication and Computational Sciences (pp. 463-471). Springer, Singapore.

[7] V. Sujatha and E. A. Mary Anita, "Detection of Sybil Attack in Wireless Sensor Network," Middle-East Journal of Scientific Research 23 (Sensing, Signal Processing and Security): 202-206, 2015, ISSN 1990-9233.

[8] S. Marian and P. Mircea, "Sybil attack type detection in wireless sensor networks based on received signal strength indicator detection scheme," in Applied Computational Intelligence and Informatics (SACI), 2015 IEEE 10th Jubilee International Symposium on, pp. 121-124, IEEE, 2015.

[9] Liu, G., Yan, Z., &Pedrycz, W. (2018). Data collection for attack detection and security measurement in mobile ad hoc networks: A survey. Journal of Network and Computer Applications, 105, 105-122.

[10] Hua, Pengwei, et al. "Energy-efficient adaptive slice-based secure data aggregation scheme in WSN." Procedia Computer Science 129 (2018): 188-193.

[11] Y. Liu, D. Bild, R. Dick, Z. M. Mao, and D. Wallach, "The mason test: A defense against Sybil attacks in wireless networks without trusted authorities," Indian Journal of Science and Technology, 2014.

[12] Ahlawat, A.and Malik, V., "An Extended Vice-Cluster Selection Approach to Improve V-LEACH Protocol in WSN", IEEE 3rd conference on Advance Computing and Communication Technology, April 2013, pp. 236-240.

[13] Babaie, S., Agaalizadeh, S. and Golsorkhtabar, M. "The Novel Threshold Based Hierarchical Clustering Method for Wireless Sensor Network", IEEE International Conference on Electronics and Information Engineering (ICEIE), August 2010, pp. 191 – 195.

[14] Bakr, B. A. and Leszek, L., "Extending Wireless Sensor Network Lifetime in the LEACH-SM Protocol by Spare Selection", IEEE 5th Conference on Innovative Mobile and Internet Services in Ubiquitous Computing, July 2011, pp. 277-282.

[15] Beiranvand, Z., Patooghy, A. and Fazeli M., "I-LEACH: An Efficient Routing Algorithm to Improve Performance & to Reduce Energy Consumption in Wireless Sensor Networks", IEEE 5th International Conference on Information and Knowledge Technology, May 2013, pp. 13-18.

[16] Chen, G., Zhang, X., Yu, J. and Wang, M. "An improved LEACH algorithm based on heterogeneous energy of nodes in wireless sensor networks", IEEE International Conference on Computing, Measurement, Control and Sensor Network, July 2012, pp. 101-104.

[17] Elbhiri, B., Fkihi, S. E., Saadane, A., Lasaad N., Jorio, A., Driss, Aboutajdine, E.R. and Morocco "A New Spectral Classification for Robust Clustering in Wireless Sensor Networks", IEEE Conference on Wireless and Mobile Networking (WMNC), April 2013, pp. 1-10.