Performance Comparison of Various Cryptographic Algorithms Along with Energy Consumption in Wireless Sensor Network

Vivek Parashar,Bharat Mishra

Abstract—Wireless sensor network (WSN), is an assortment of sensor nodes placed in vicinity to each other which may result in higher communication leads to the failure of nodes. They can overcome node failure through easy exploiting another routing path. Energy utilization is one of the prominent issues in WSN to maintain the lifetime of the network. Entire network life span is depending on proficient energy exploitation in the sensor network. In this paper, the challenges, limitations, and characteristics of WSN have been discussed. There are various cryptographic algorithms available to surpass the safety of the network by the detailed analysis of the algorithms, the encryption, and decryption of the different algorithms has been taken into consideration. The nodes are placed in a manner so that transmission can be performed securely over the network. The results have shown that the data sent securely from the source to the Base Station. We have used a MATLAB simulator to differentiate the various algorithms. The certain parameters are shown in this paper such as energy and packet sent to the Base Station.

Index Terms—WSN, Routing Protocols, Security, Cryptographic Algorithms, Energy consumption

1. INTRODUCTION

WSN is an essential part of the Internet of Things (IoT) depicted below in figure 1 redrawn from [1]. Many applications in IoT require WSN as a key element. The majority of WSN applications require transmission or processing of real-time multimedia and other data, including the healthcare system, target monitoring, and numerous others. In WSN, sensor node has little memory capacity, and the buffer resources utilized for routing are noticeably few, however genuine time multimedia have a huge amount of data. The data travel through various intermediate nodes to reach to sink node in a multi-hop manner since all nodes are creating data which may lead to conjunction in a network. Therefore, some mechanism is required to avoid congestion in the network. Transmission delay made within the network due to congestion will lead to failure of a system or delay in giving the desired output from the system. As we understand, the sensor nodes are normally controlled through the battery, nodes in congestion consume massive energy due to which a few nodes get power exhausted earlier than the other nodes, which may lead to reduce the overall lifetime of the system [2].

In the paper, there are various sections and their description is explained as: in section II, there are various characteristics of WSN to understand the network. In section III, the advantages of WSN are studied to know the usage of the network. In section IV, applications are described to show the practical utilization of WSN. In section V, certain issues of security are illustrated to upgrade the overall performance of the WSN network and section VI, show the goals of these security requirements. In section VII, some communication protocols are explained which is applied on WSN for implementing the task. In section VIII, literature survey has given to show the previous work done performed in this field. In section IX, challenges and limitations of WSN are mentioned to understand the gaps in the work and what is to overcome by our work. The challenges are overcome in section X in the form of the proposed methodology. In section XI, the result analysis has been performed and display in the form of graphs. Lastly, the conclusion mentioned showing the overall work of the paper.

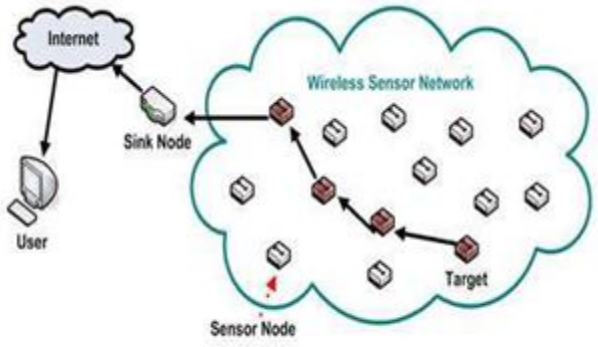

Figure. 1. WSN environment

2. CHARACTERSTICS OF WSN

The four important WSN characteristics are mentioned below [3]

2.1 Dynamic Network Topology

In this network topology, the configuration of nodes changes depends on the network requirement, they may join or leave

- *Vivek Parashar is a research scholar from MGCGV, Chitrakoot (MP), India and Assistant Professor, Amity University Madhya Pradesh, India, PH-8878644486. E-mail: vparashar@gwa.amity.edu.*
- *Bharat Mishra is Associate Professor department of Physical Sciences MGCGV, Chitrakoor (MP), India, PH-9425888134.*

as an when required, based on node failure, channel fading or energy depletion. Therefore, the network remains ever-changing in WSN.

2.2 Application Specific

WSN can be deployed based on the requirement of an individual or organization for a specific requirement and time duration. Few of them already discussed in previous sections.

2.3 Energy constrained

Nodes may or may not be moveable and are having limited energy. Nodes must perform computation and transmission and reception of signals which consumes IoT of energy which make them to fail after some time [4].

2.4 Self-configurable

Nodes are usually placed randomly without any specific plan. Therefore, nodes have to be self-configurable according to the real time situation of the network [5].

3. ADVANTAGES OF WSN

Due to numerous uses, WSNs has changed the perception to see the world around us. WSN is fitting in almost every part of our lives. We have enlisted few of the benefits [6] of WSN.

3.1 Ability to Withstand in Adverse Environmental Conditions

As we know that the sensor nodes can be placed anywhere and can withstand in harsh environment also. WSN can be applied in difficult locations like forests, mountains, fireplace detection, deserts, seismic monitoring.

3.2 Ease to Deploy

Areas like forests, war fields, places in and around volcano or water body are very difficult to monitor, but with the help of sensors we can easily do it and the sensors can easily be placed by throwing from an airplane or drone in random order and nodes will automatically connect each other.

3.3 Ability to reconfigure themselves

In WSN sensor nodes are placed in the vicinity. WSN nodes can overcome failure, in case of dead or destroyed nodes by exploiting other routing path. For instance, during war or natural calamity, if few nodes get destroyed, the system will keep working, due to the reconfiguration capability of WSN nodes which reconfigures the system to keep it alive.

3.4 Ability to work in versatile and rough environment

Many times, it is not possible to deploy wired network due to high infrastructure cost or due to an adverse working environment, in such cases WSN can easily be deployed. For instance, setting-up of a wired network in flooded area or on a battlefield is not viable. WSN can be accommodated in such areas because it is cheap and require no infrastructure.

3.5 Mobility of Nodes

When WSN nodes are placed inside the sensing area, nodes have the capability to configure themselves and create a network, discover nodes and formulate network, create a multi-hop broadcast in a small amount of time [7]. Nowadays, since the world is getting mobile therefore mobility of nodes has been exploited deeply so that no event will remain unattended, a lot of Advance Protocols and architectures are available which are capable of dealing with those real-time movements of nodes.

3.6 Unattended Operation

WSN can work unattended with no human intervention. This reduces the labor requirements and hence reduce the cost. The system will work with more accuracy and reduce the rate of error. Since no human is required the date will be gathered on time and accuracy. Therefore, such systems are more helpful to manage Home, industry, field monitoring, etc.

3.7 Ability of Collect Accurate Data

WSN are designed to collect the data for the specific application. The nodes are placed in the vicinity or at the location of the event which helps them to collect accurate data and reduce noise

4. APPLICATIONS OF WSN

Figure 2 redrawn from [8] show various applications of WSN, WSNs are presently being utilized in almost all fields from homes to industrial monitoring [9] by incorporating cameras and sensors which can see and identify the problem. You can control the problem from far end manually or even system can take decision based on predefined rules, Medical investigation can be made more effective with the advent of sensors and virtual reality [10] in which you can even feel of being a part of operation performed on the actual ground. WSN make military operations more effective [11] by include surveillance and target tracking of hostile environments, snipers and intruders and can make areas accessible which cannot be tracked otherwise. Sensor networks have vast applications in industry as well, they could be utilized for monitoring hazardous chemicals, furnaces, automobile industry, mining industry etc. In Industry robotic arms equipped with sensors are used to perform the specific tasks with the required accuracy. Sensor networks can be used to detect and predict the environmental changes and to warn us as well, like early fire warnings in forests, seismic data collections, flood and landslide detection [12]. WSN is used in agricultural applications [13] where various decisions like irrigation, fertigation, identifying the best suitable crop based on soil type, atmospheric pressure, climatic conditions can be detected and analyzed, and decisions are taken accordingly to maximize production.

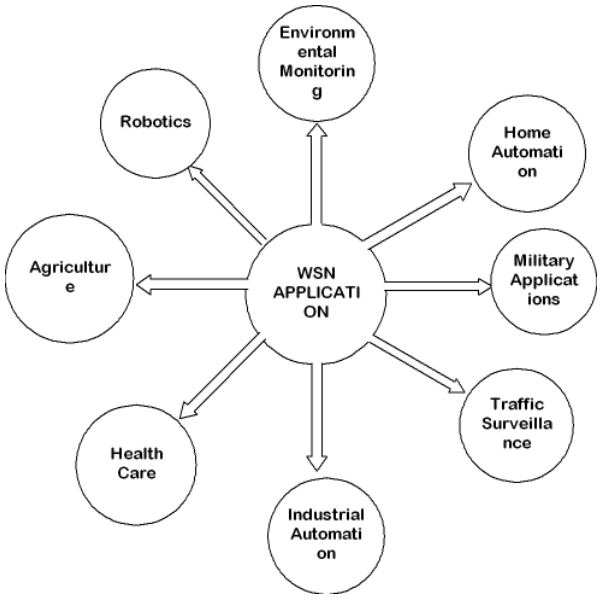

Figure. 2. Applications of WSN

5. SECURITY ISSUES IN WSN

WSN is formed by deploying sensor nodes. The architecture and the location of nodes are application-specific. Since all the nodes try to transmit data towards the sink node, which is vulnerable to attack by intruders hence threat always exist in WSN. Here we are discussing three main factors which are affected by a breach of security [14].

5.1 Data Availability

It ensures that the availability of data remains consistent even under DOS attack. Data availability is an important aspect because it is of primary importance to maintain an operational network. Availability ensures that a sensor node in WSN remains always dynamic in the network to satisfy the usefulness of the network [15].

5.2 Data Authentication

It ensures that the data during transmission in WSN remain intact and not been spoofed throughout the transmission. In order to ensure the data integrity symmetric or asymmetric transmission mechanisms is used, in which both sender and receiver share the same secret keys [17].

5.3 Data Freshness

WSN is used to share or transmit the real time data for storing or processing. In order to ensure data freshness, the hope count or time to live(timestamp) field is incorporated in each packet. It will ensure that no unwanted or garbage data remain in the system [20].

6. SECURITY REQUIREMENTS AND GOALS OF WSN

WSNs are specific kind of ad-hoc network. WSN requires Security to defend the attack and stop intruders from accessing the network and data. The principle objectives are insinuated too known security destinations comprehensive of confidentiality, integrity, authentication and availability (CIAA). The other requirements are Data freshness, Time-synchronization, Self-association, and Secure Localization [16]. The exact portrayal is given underneath.

6.1 Data Confidentiality

It ensures the privacy and security of data by using cryptographic algorithms . Cryptography strategies are used to offer confidentiality. It is one of the most essential trouble of the network security. Confidentiality ensures the safety of messages from a passive attacker with the goal to keep every sensor data intact and secure even at the individual sensor level. It ensures that a given message can't be comprehended by method for everyone separated from the well-known recipients. This is the most essential issue in network security. For the secure report, encryption is used. Data is encrypted with the mystery key that best affirmed customers have Public sensor facts need to moreover be encrypted to a couple of degrees to safeguard contrary to traffic analysis attacks.

6.2 Data Authentication

It ensures the trustworthiness, quality of the message starting from source to destination. Attacks in sensor networks not only effects the packets, but it can mix the other malicious information to the packet. It guarantees that a malicious node can't go up against the presence of a trusted system node. Data authentication empowers the receiver to check the date received is similar to what is being dispatched to him. Authentication can be confirmed by the report of both sender and receiver based on the shared secret key

6.3 Data integrity

It guarantees that data packets received by the destination are exactly that sent by the sender and any intruder can't adjust that packet in between [18]. Data integrity in sensor networks is expected to make certain the reliability and quality of the data and insinuates back to the sender that the data is not tempered. Regardless of this, it doesn't mean the data is intact. The adversary can change the data which are available within the network. It can inject fake data into the network that makes the system unstable.

6.4 Data Availability

It ensures that data will remain available all the time, even at the time of attack such as DOS-attack. Availability ensures that data remain available for network and nodes remain active in any adverse situation [19]. The secondary desires are

6.4.1 Data Freshness

It ensures that the data received through the receiver are real time data and no node in the network will reply the old statistics [20]. It is executed with the aid of the use of mechanisms like hope count or time-stamp to every data packet. Data freshness in short can be viewed as message requesting: inclined and solid freshness. Weak freshness delivers packets but does not answer clearly about the hope count and latency of the message. Strong freshness, however, gives consolidate information about entire request-response. Sensor necessities require slanted freshness, while solid freshness is required for time synchronization in the network. To guarantee that no old message required a timestamp may be acquainted with the packet.

6.4.2 Self –Organization

A WSN is an Ad-hoc network, in which each sensing node is free and flexible having the capability of self-organization and self- recovery, consistent with distinctive. There isn't generally any constant or fixed infrastructure for operation in a bounded or open area, this makes WSN system vulnerable to attack. The dynamic idea of a WSN makes it occasionally unrealistic to establish any preinstalled shared key system the various nodes and the base station.

6.4.3 Time-Synchronization

In WSN applications, sensors usually transfer data at specific time intervals following time-synchronization. The older algorithms like network time protocol and global positioning system are not enough to have efficient and faster data transfer. In order to avoid the delay during synchronization, we may use Reference Broadcast Synchronization (RBS) or Timing-Sync Protocol (TSP). [21]. An additional collaborative sensor network may also require association synchronization for tracking packages.

6.4.4 Secure Localization

In WSN each sensor node is needed to breeze up in the network as it ought to be and routinely to discover the area of the fault [22].

7. COMMUNICATION PROTOCOLS

WSN consists of layered structure much like wired community structure [23] [24]. The characteristics and features of their every layer are given below.

7.1 Physical Layer

This layer deals primarily with hardware and signalling. This layer majorly dealt with frequency-period, data rate, data encryption, modulation, sign detection, and signal detection.

7.2 Data Link Layer

DLL ensure interoperability. It performs data exchange within the network. This layer is primarily responsible for multiplexing, error detection, Prevention of Collision of packets, repeated transmission, and so on. A few researchers have worked on the practical utilization of public key cryptography agreeable code appropriation to frame calm key all through a network establishment and conservation.

7.3 Network Layer

This layer emphasis on effective routing. It finds the best possible path in the network. This layer oversees routing the data from the sensing node to the destination node through intermediate nodes(sink or base station). The LEACH and PEGASIS are the conventions are extensively utilized strategies to keep the power utilization (energy of sensor) altogether that it enhances the lifespan of sensor nodes. LEACH offers cluster essentially based totally transmission even as PEGASIS is chain protocol for routing, WSN makes use of data-centric protocols and ID-based protocols. All nodes in WSN network can work as a router and help the network in creating secure routing protocol which uses a broadcast communication scheme. User can deploy various encryption and decryption techniques for secure routing in the network.

7.4 Transport Layer

Transport Layer offers delivery of information from origin to final destination (end-to- end) with reliability. It also handles the conjunction in the network. It works like an Internet layer in TCP/IP protocol suite.

7.5 Application Layer

The foremost responsibility of Application Layer is to ensure the delivery of data to the lower layer recipient by guarantying smooth flow of information. This layer accounts for data collection, control and preparing of the data by means of the application programming system to procure tried and true outcomes. SPINS (Security Protocols in sensor Networks) and Localized Encryption and Authentication Protocol (LEAP) is a key administration protocol for sensor networks. It works with various keying mechanisms (Group Key, Cluster Key, and Pair Canny Shared Key). The security mechanisms will be discussed in detail in the next section.

8. LITERATURE SURVEY

In [25] the author has focused on increasing the lifetime of a WSN network. To achieve longer lifetime two mechanisms were used, first was optimal sensor node deployment and second was Wireless Energy Transfer(WET) scheduling. In order to achieve the immortality in the network two step procedure was followed. First, the situations for which the WSN could be immortal was established based on this the node deployment algorithms for ideal node deployment was designed. Once the optimal node deployment was achieved the WET scheduling algorithm was implemented. Theoretically the WSN seems to be immortal with the help of optimal node deployment and WET scheduling. The simulation results shown that the requirement of node due to optimal node deployment policy reduced with the immortal lifetime of the network.

Dina S. Deif, et al. [2017] in [26] discussed, the issue of node arrangement with minimum cost and high reliability were discussed. The reliability of WSN network is important from application point of view if the network fails the entire system may crash. The system may fail due to node failure, transmission failure, etc. In this paper minimum cost reliability constraint sensor node deployment(MCRC-SDP). The MCRC-SDP is considered an NP-Complete problem. To solve the problem ant colony optimization with local heuristics was used the simulation results shows a great change in the reliability with reduced cost.

Gudivada, R.B.et al. [2018] in [27] focused on minimizing energy consumption without compromising with security. WSN supports both symmetric key cryptography and public-key cryptography for security in the network. Public-key cryptography provides better security than symmetric key cryptography as it provides the unique key to every node in the network, but it consumes more energy than symmetric key cryptography which is vulnerable to cryptanalysis. In this paper, ECC-based public key cryptography is used to generate the public-key to identify the nodes uniquely and to establish symmetric-key between the pair of nodes. In order to reduce the frequent key generation, the symmetric Diffie-Hellman key

renewal scheme was used to renew the keys and to reduce the energy consumption during key generation.

Kyoungsoo Bok et al.[2016] in [28] improved version TinyMD5 of MD5 has proposed, that convert the sensed data using hash- function.TinyMD5 divides the data to make decryption difficult and then to send data from multiple paths for better security.

Duan Jiaying et al. [2016] in [30] used optimal WSN node arrangement for monitoring high speed railway system was discussed. The Railway carries a large number of people, hence the system must be secured and fast enough to transfer the information at real-time. The goal of designing such network is to find out the optimal deployment scheme(based on number of relay node and their deployment) for maximizing the utilization efficiency defined as the network lifetime divided by the number of deployed sensors [29].

Mauricio Postigo-Malaga et al. [2016] in [31] displayed an architecture has been proposed to eliminate handover. In WSN the communication between the nodes are coordinated by a sink or coordinator node, the arrangement of a coordinator with other node is called personal area network (PAN). When any node moves from one PAN to another PAN it performs handover. In the proposed architecture the need of handover is abolished. In the proposed architecture two PAN configuration was considered, one which is responsible for communication between sensor node and access point(AP) and other forming backbone network between access point and coordinator node. The result of such experiment is very satisfactory in comparison to other communication methods.

9. CHALLENGES AND LIMITATIONS OF WSN

In WSN sensor nodes have limited transmission capacity, storage space, and power. This will put a great challenge in front of developers to manage data transmission, device networking strategy for unicasting or multicasting of data, device techniques for data aggregation so that lifetime of the network can be increased. The network lifetime is the key property used for differentiating the execution of any sensor network. A span time of the network is resolved by means of residual energy of the machine, therefore major and most extreme basic endeavour in WSN is the proficient adventure favorable position of Energy sources. Literature indicates the power efficiency is offered in WSNs using any of the accompanying components: power protection instrument, Power conservation system, energy efficient routing, and power harvesting mechanism. Apart from the limitation of sensor node WSN network is prone to security threats related to communication and physical safety because they may be placed in areas which are unattended by anyone. Problems like DOS-attack in which victim node receives unwanted traffic, which exhausts the resources it is entitled to. In Sybil- attack, a node tries to forge the identity on another node result in degrading the security and integrity of data. Attack on information during transmission of data, in this the sending information from one node to others may be spoofed or altered or may be vanished. Blackhole/sinkhole attack, in this a malicious node act as a black hole it relays a message in network informing other nodes that best route goes through him and one's nodes opted the path through him to manipulate or copy the data. In wormhole attack, the attacker node receives the signal from transmitting node who wants to communicate within the network and tunnel it to the node which may not be reachable and pretends that this is the right path of communication this will result in the failure of communication. These are not only threats, there are other threats as well leads to communication failure in WSN Hence the requirement of the security mechanism in WSN is very important.

9.1 Energy Aware Routing

The goal of routing in WSNs is to hunt and keep routes in WSNs. Routing challenge with reference to WSNs are Node diffuse, Link heterogeneity, Data reporting model, Scalability, Energy utilization without losing accuracy, network dynamic transmission media, Coverage, Data aggregation, QoS, Connectivity [32].

10. PROPOSED METHODOLOGY

We have studied various algorithms for this purpose, but we have taken only four prominent algorithms for comparison, in our research work because of their extensive use and limitations of another algorithm for implementing in WSN. In proposed methodology, detail considerations of these algorithms are show the effectiveness of the algorithm. DES, AES, RSA and NTRU algorithms are analyzed in terms of key generation, encryption and decryption. A WSN is a specific network which has various impediments contrasted with an ordinary computer network. Due to these restrictions it is difficult to straightly make use of the provided security approaches to WSNs. Therefore, in order, to build up invaluable security methods whilst borrowing the ideas from the current security approaches, it is necessary to understand and appreciate these restrictions first. In this section we speak about various algorithms for the security of WSNs [33] [34].

10.1 Data Encryption Standard (DES)

International business machine(IBM) has designed Data encryption standard(DES) which is a symmetric block cipher uses a 56-bit key to encipher/ decipher a 64-bit block of data. The key is continually appeared as a 64-bit thwart, each eighth bit of which is in secret. It was the essential encryption algorithm allowed by the U.S. government for open introduction. This ensured DES was instantly gotten by wanders, for instance, financial administrations, where the necessity for strong encryption is high [35]. The straightforwardness of DES similarly watched it used as a piece of a wide extent of installed frameworks, keen cards, SIM cards and network devices including encryption like modems, set-top boxes and switches. In any case, DES isn't secure. DES, the Data Encryption Standard, can no longer be measured safe. While no major flaws in its innards are known, it is essentially not enough because its 56-bit key is too small.

10.2 Rivest-Shamer-Adleman (RSA)

Rivest-Shamer-Adleman is the most typically utilized open key encryption estimation. RSA can be used to send an encoded message without a substitute exchange of emanate key [36] [37]. It can equivalently be used to sign a message. In RSA, this asymmetry relies upon the sensible trouble of figuring the

consequence of two broad prime numbers, the ascertaining issue. The security of RSA computation relies upon the inconvenience of figuring of tremendous numbers. RSA is an asymmetric calculation and plays a key capacity in broad daylight key cryptography. It is extensively utilized as a part of electronic communication protocols.

10.3 Advanced Encryption Standard (AES)

AES uses 128 bit key for security, it ensures that is is very difficult to break the key even in billion years even on snappiest supercomputer. AES-128 encodes messages in lesser time and devours less battery power [38]. In like manner it is clear to execute in hardware and s/w and likewise in constrained circumstances like keen cards. NIST in the reference record closed and educated that each one as for the 3 key-lengths (128- bit, 192- bit and 256- bit) of AES exhibit sufficient encryption until past timetable year 2031. AES is a symmetrical encryption calculation by and large sensible for encoding larger part of data. It tackles a shot at a 4x4 fragment genuine demand lattice of bytes, named the state (varieties of Rijndael with a bigger piece estimate gage have extra segments in the state). AES is block cipher. It has variable key length of 256, 192, or 128 bits. It encodes data bits of 128 bits in 10, 12 and 14 round dependent upon the key size. AES encryption is quick and elastic; it can be associated inside the extraordinary platforms.

10.4 N th Degree Truncated Polynomial Ring (NTRU)

NTRU encryption scheme is a lattice-depend public key cryptosystem that give highest speed key creation, encryption, and decryption. It's very well-known in electronics industry [39]. Polynomials are exploited with a purpose to generate key pair. Modular operation is exploited to encrypt messages the use of encryption keys. Brute Force attack and meet in-the middle attacks are solved by means of NTRU. Lattice reduction and selected cipher text attacks have damaged the NTRU. It's still secure to many attacks but there's a tradeoff amid safety and overall performance which make it inclined. A pear to pear (P2P) public key cryptography (PKC) to secure mobile communication. It offers authentication, confidentiality, and integrity needed for mobility gadgets. NTRU is exploited for PKC. It performs key technology, encryption, and decryption. It is positioned that NTRU offer identical safety equated to RSA. Key exchange is complete via a deffie-hellman mechanism. Encryption is then accomplished the usage of AES-Rijnadeal algorithm as it holds less NTRU keys. Encrypted messages are then communicated between mobile users. In the table 1, the detailed description of the algorithms is performed in terms of advantages and disadvantages related to them.

TABLE 1: DESCRIPTION OF ALGORITHMS

Algorithm	Advantages	Disadvantages
DES	• DES is difficult to attack and crack since the measure of rounds are sufficient for encoding the message. • DES is quicker when contrasted with another Algorithm. • DES has abnormal state of security. • It is totally indicated and straightforward. • It is versatile to various applications. • DES can be approved and Exportable.	• 2 selected i/p to an S-box can make a similar o/p. • The reason for beginning and last stage isn't clear. • Specialists have discovered a shortcoming in the plan of the cipher generation.
AES	• It is most strong protocol for security. • It utilizes higher length key sizes, for example, 128, 192 and 256 bits for encryption. • It is most normal protocol of security utilized for wide different of applications. • It is a standout amongst the most spread business and open source arrangements utilized everywhere throughout the world.	• It utilizes excessively straightforward logarithmic structure. • Each block is constantly encoded similarly. • Difficult to perform implementation with programming. • AES in counter mode is mind boggling to execute in programming taking both execution and security into contemplations.
RSA	• RSA calculation is protected and secure for its clients using complex operations. • RSA calculation is difficult to break since it includes factorization of prime numbers which are hard to factorize. • RSA calculation utilizes people in general key to scramble information and the key is known to everybody, thusly, it is anything but difficult to share the general population key.	• RSA calculation can be moderate in situations where vast information should be encoded by a similar PC. • It requires an outsider to confirm the unwavering quality of open keys. • Information exchanged through RSA calculation could be bargained through go between who may temper with people in general key framework.
NTRU	• More productive encryption and decoding, in both equipment and programming usage. • Considerably speedier key formation. • Low memory utilizes enables it to use in applications, for example, cell phones and Smart-cards.	• NTRU is more up to date as well, and for a similar level of security requires longer keys and cryptograms (in bits) than RSA and ECC.

11. RESULT ANALYSIS

We performed the simulation on the various parameters. For the security there are some analysis performed to demonstrate the technique. For the simulation we have used MATLAB. Comparisons of various DES, RSA and NTU algorithms are shown below in figures 3 to figure 6. In the table below, the simulation parameters are mentioned with their values which are used in the experiment:

TABLE 2: SIMULATION PARAMETERS

Parameters	Values
Energy for Transmitter and Receiver	50 nJ/bit
Energy magnification for free space	10 pJ/bit/m2
Multi path's Energy	0.0013 pJ/bit/m2

magnification	
Initial Energy of Nodes	0.5 J
Energy for Data Aggregation	5 nJ/bit/message
Size of Packet	1K bits
No. of nodes	200
Size of Network	100m x 100m
Position of BS	50m x 50m
Distribution of nodes	Uniform

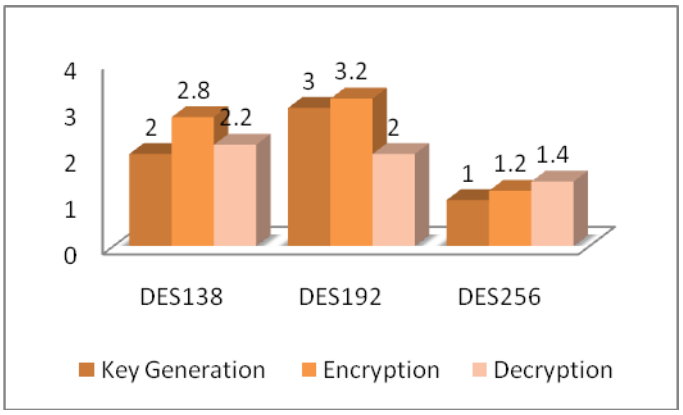

Figure 3. Time Comparison between Various DES Algorithms

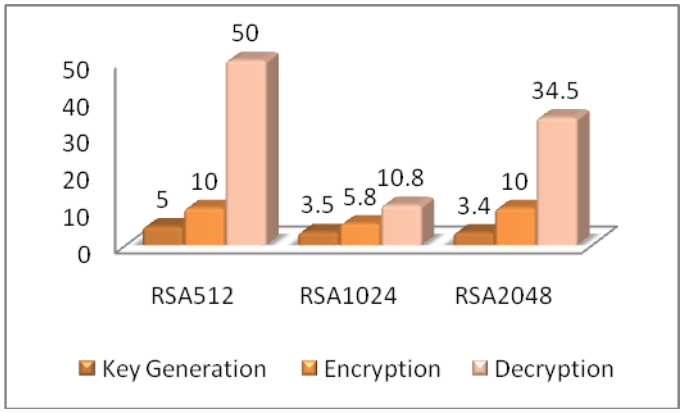

Figure 4. Time Comparison between Various RSA Algorithms

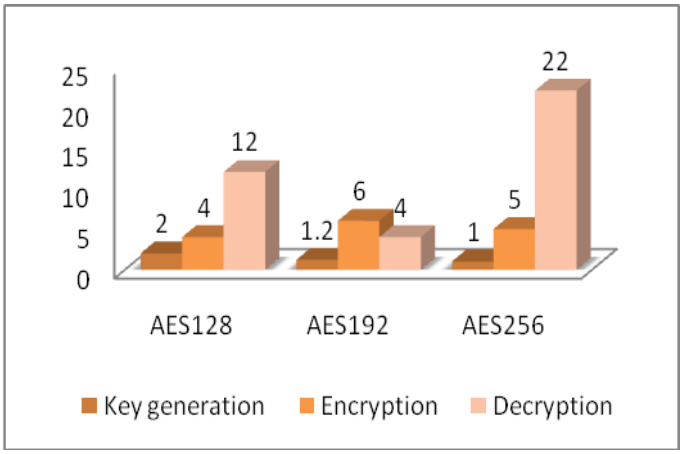

Figure 5. Time Comparison between Various AES Algorithms

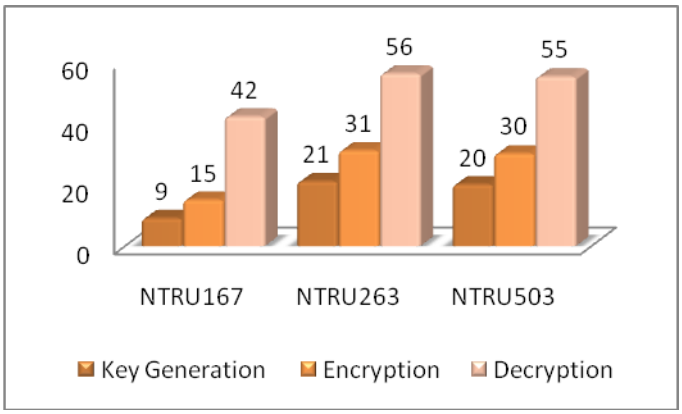

Figure 6. Time Comparison between Various NTRU Algorithms

The figure 7 below shows the data transmission from source to destination using above algorithms. It shows that there are different sensor nodes in the network and separation the network into smaller segments and afterward transmit the data from the source node to the base station.

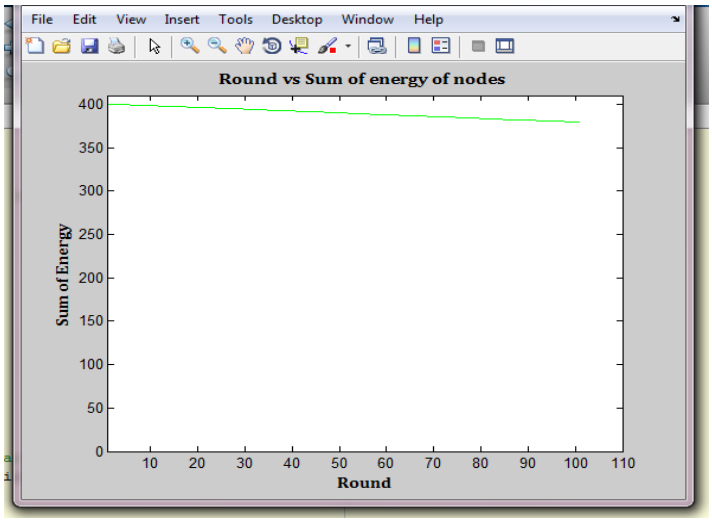

Figure 7. Sensor Nodes in the network

In the figure 8 below, we show that with increase in the

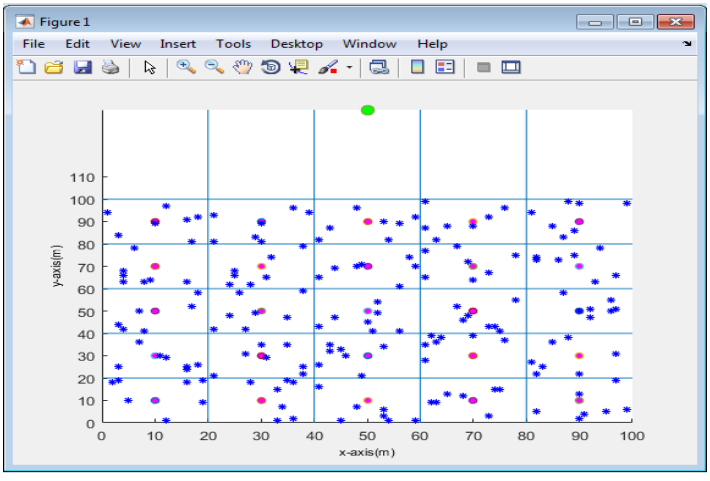

Figure 8. Round vs Number of packets sent to BS

number of rounds our more packets delivered to the base station, which improves the efficiency of the network. The figure 9 below shows that the sum of energy of all nodes in the network decrease with the number of rounds because the energy of the nodes decreases due to the communication of node or actions performed by them for the transmission of data from one node to another. Energy consumption of each node are calculated and illustrate that the energy decrease with the number of rounds increase.

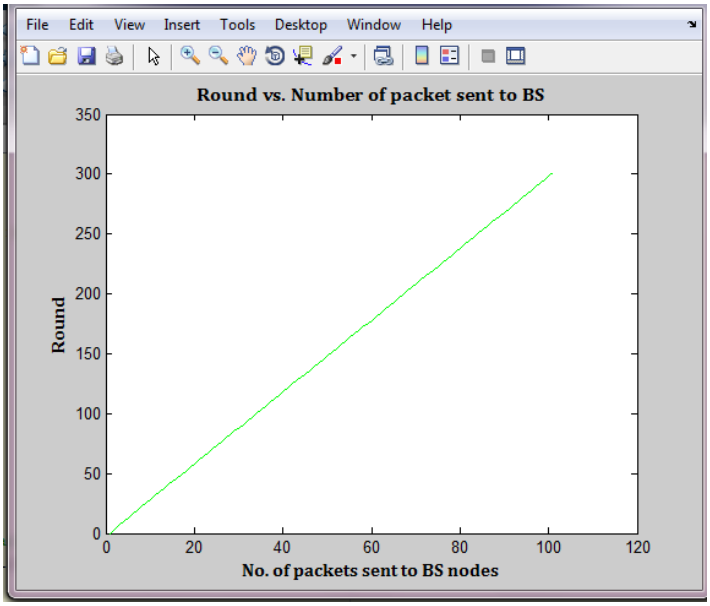

Figure 9 Round vs Sum of energy of nodes

In the figure 10, energy consumption graph shows the energy at each node. Energy decrease after each round and it will run 2000 iterations

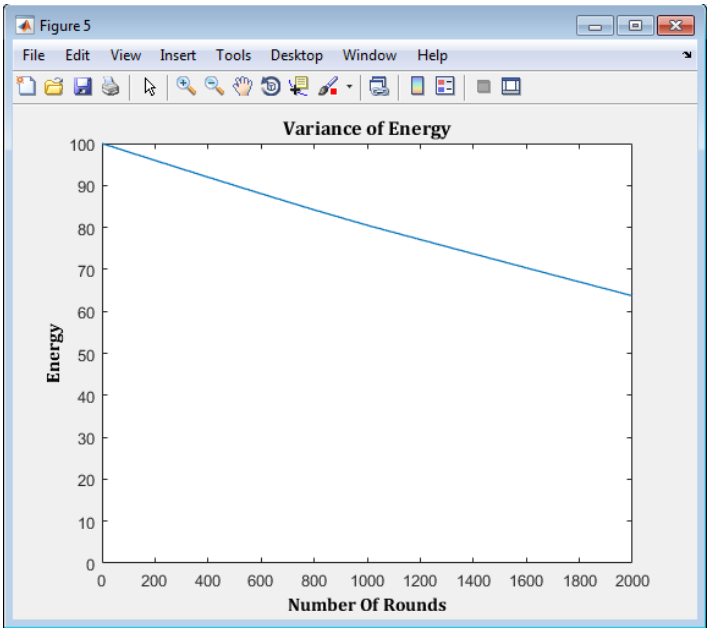

Figure 10. Round vs Sum of energy of nodes

Figure 11, shows the variance of lattice-energy ,calculated with the number of rounds. Shortest path algorithm is used to reduce the energy consumption of the nodes.

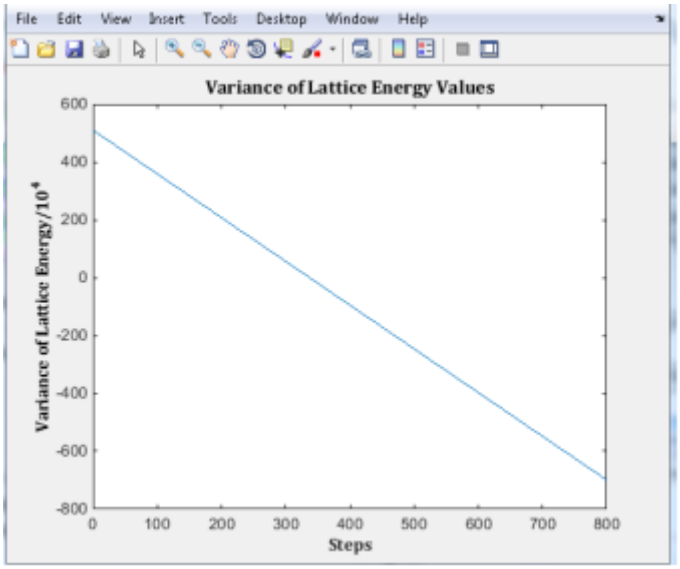

Figure 11. Variance of lattice energy

Figure 12 shows the energy consumption at different number of nodes and demonstrate that less number of nodes required more energy to forward the data towards the base station.

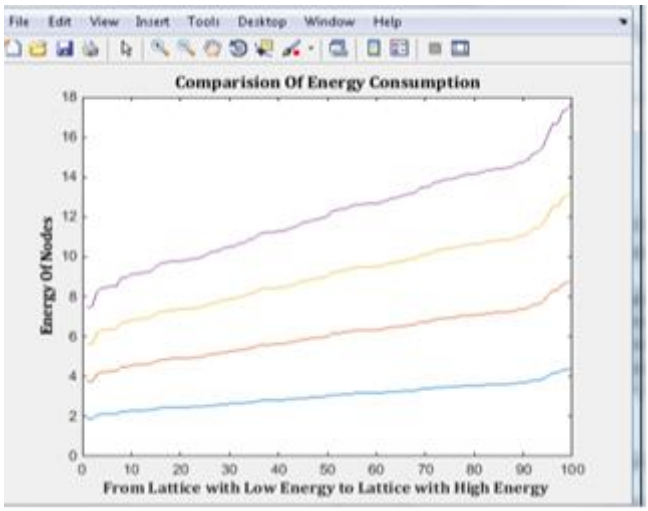

Figure 12. Energy consumption in each lattice

12. Conclusion

Wireless Sensor Networks (WSNs) include sensor nodes that can be deployed in a subject or specific-area and interconnected with a wireless communication network. Each of those scattered sensor nodes has what it takes to collect data, fuse that insight and forward again to the sink/base station. The routing protocols available for wired network can't be utilized here because here in WSN, nodes are battery controlled. Because of this, WSN should be the energy proficient. Whole network lifetime is depending on capable energy usage in the sensor network. From the detailed analysis, it is shown that AES algorithm is better than data

encryption standard s(DES), Rivest–Shamir–Adleman (RSA) and NTRU. Then the node deployment performed by the cluster formation to the base station and cryptographic techniques can be applied to secure the transmission in the network. In the paper, different techniques are used to show the energy consumption comparison and show that different nodes consume the different amount of energy.

REFERENCES

[1] Gogu, A., Nace, D., Dilo, A., & Meratnia, N. (2011). Optimization problems in wireless sensor networks. In Proceedings of the international conference on complex intelligent and software intensive systems (pp. 302–309)

[2] Qi Li, Zongwu Ke , Duanfeng Xia & Sun Yuxia (2013), A Routing Protocol for Wireless Sensor Networks with Congestion Control,Communications and Network, ISSN: 1949-2421 2013, 5, 156-160

[3] Yong-Min, L., Shu-Ci, W. & Xiao-Hong, N.(2009) The architecture and characteristics of wireless sensor networks, IEEE International Conference on Computer Technology and Development.. Kota Kinabalu, Malaysia; :561–565.

[4] Björnemo,E.(2009), Energy constrained wireless sensor networks: Communication principles and sensing aspects, Dept. Eng. Sci., Uppsala Univ.

[5] Clouqueur Thomas ,Phipatanasuphorn Veradej ,Ramanathan Parameswaran & Saluja K. Kewal (September 28, 2002) , Sensor deployment strategy for target detection, Proceedings of the 1st ACM international workshop on Wireless sensor networks and applications, Atlanta, Georgia, USA.

[6] Gupta, S. K. & Sinha, P.(2004), Overview of Wireless Sensor Network: A Survey, International Journal of Advanced Research in Computer and Communication Engineering, Vol. 3, Issue 1.

[7] Basagni, S., Carosi, A., and Petrioli, C. (2008). Mobility in wireless sensor networks. In Algorithms and Protocols for Wireless Sensor Networks, A. Boukerche, Ed. Wiley Series on Parallel and Distributed Computing. John Wiley & Sons, Inc., Hoboken, NJ, Chapter 10, 267--305.

[8] Halil, Y., Kent, T. Kan, C., & Mohammed, E., (2017), "A Survey of Network Lifetime Maximization Techniques in Wireless Sensor Networks", IEEE Communications Surveys & Tutorials, 19(2):828 – 854.

[9] El Brak, I. S.(2012), wireless sensor network in home automation network and smart grid,Complex Systems , International Conference on computational Science (5-6 Nov. 2012) 1-6.

[10] Chen, M.,Gonzalez, S.,Vasilakos, A. and Cao, H.; Leung, V.C.M.(2010), Body Area Networks: A Survey. Mob. Netw. Appl. , 16, 171–193

[11] Durisic, M. P., Tafa, Z., Dimic G. and Milutinovic V(2012), A survey of military applications of wireless sensor networks, Proc. MECO, pp. 196-199.

[12] Arampatzis, T., Lygeros, J. & Manesis, S.(June 2005), A Survey of Applications of Wireless Sensors and Wireless Sensor Networks, 13th Mediterranean Conference on Control and Automation Limassol.

[13] Kassim, M.R.M, & Harun, A.N. (2016), Applications of WSN in agricltural environment monitoring systems, International Conference on Information and Communication Technology Convergence (ICTC), pp. 344-349, 2016.

[14] Singla,A., & Sachdeva, R.(2013).,Review on security issues and attacks in wireless sensor networks, international Journal of Advanced Research in Computer Science and Software Engineering, vol. 3, no. 4, pp. 529–534.

[15] Yelong Shen,Ning Xi,Qinigqi Pei,Jinafeng MA,Qijian XU & Zuoshun Wu (2011), Distributed Storage Schemes for Controlling Data Availability in Wireless Sensor Networks,Seventh International Conference on CIS,sanya,Hainan.China,pp 545-549.

[16] Redwan, H. & Kim, K. H.(Nov 2008), Survey of security requirements, attacks and network integration in wireless mesh networks, in New Technologies, Mobility and Security, NTMS '08. , pp. 1-5.

[17] Cui, J., Shao, L., Zhong, H. et al (2017).Data aggregation with end-to-end confidentiality and integrity for large-scale wireless sensor networks,Peer-to-Peer Netw. Appl.,springer US, 1936-6442.

[18] Patil, S., D. V. K. B. P, Singha, S. and Jamil, R. (2012). A Survey on Authentication Techniques for Wireless Sensor Networks, International Journal of Applied Engineering Research, vol. 7.

[19] Li,J., Andrew,L.H., Foh,C.H., Zukerman,M., Chen,H.H.(2009),Connectivity coverage and placement in wireless sensor networks, Sensors, vol. 9, no. 10, pp. 7664-7693.

[20] Kang, K. D., Son, S. H., and Stankovic, J. A. (2004). Managing deadline miss ratio and sensor data freshness in real databases. IEEE Transactions on Knowledge and Data Engineering 16(10): 1200–1216.

[21] Lasassmeh, S.M.& Conrad, J.M.(2010), Time synchronization in wireless sensor networks: A survey. Proceedings of IEEE SoutheastCon , Concord, NC, USA, 18–21 March 2010; pp. 242–245.

[22] Apkun, S.,Rasmussen, K. & Ajali, M.(2008) ,Secure Location Varification with Hidden and Mobile Base Station,IEEE Trans.Mobile Computing,Vol 4,pp 470-483.

[23] Pesch, D.(2017), Communication protocols for wireless sensor networks, Presented Slides in 3-Workshop on RF Wireless Sensor Networks Research in Ireland, Dublin, Ireland.

[24] Al-Karaki, J.N. & Kamal, A.E.(2004) , Routing techniques in wireless sensor networks: a survey, IEEE Wireless Communications, vol. 11, no. 6, pp. 6-28.

[25] Rong Du, Carlo Fischione, Ming Xiao (2017),Joint Node Deployment and Wireless Energy Transfer Scheduling for Immortal Sensor Networks,15th International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks.

[26] Deif,D.S and Gadallah,Y(2017). ,An ant colony optimization approach for the deployment of reliable wireless sensor networks, IEEE Access, vol. 5, pp. 10744–10756.

[27] Gudivada, R.B., and Hansdah, R.C.(2018), Energy Efficient Secure Communication in Wireless Sensor Networks, 2018 IEEE 32nd International Conference on Advanced Information Networking and Applications (AINA), Krakow, 2018, pp. 311-319.

[28] Kyoungsoo Bok, Yunjeong Lee, Junho Park, and Jaesoo Yoo, "An Energy-Efficient Secure Scheme in Wireless Sensor Networks," Journal of Sensors, vol. 2016, Article ID 1321079, 11 pages, 2016.

[29] Lin, Y., Zhang, J., Chung, H.S.-H.,Ip,W. H.,Li,Y. & Shi,Y.H., (2012), An ant colony optimization approach for maximizing the lifetime of heterogeneous wireless sensor networks, IEEE Trans. Syst. Man Cybern. C Appl. Rev., vol. 42, no. 3,pp. 408-420.

[30] Jiaying Duan,Tianyun Shi, Lv Xiaojun & Li Zhi(2016), Optimal Node Deployment Scheme for WSN- Based Railway Environment Monitoring System, The review process for the

28th Chinese Control and Decision Conference.
[31] Postigo-Malaga, M., Supo-Colquehuanca, E., Matta-Hernandez, J., Pari Lizardo , Efra´ın Mayhua-Lopez(2016) ,Vehicle Location System and Monitoring as a Tool for Citizen Safety Using Wireless Sensor Network, IEEE ANDESCON, pp 1-4.
[32] Wei, D., Jin,Y., Vural,S. & Moessner, K.(Nov 2011), An Energy-Effcient Clustering Solution for Wireless Sensor Networks," IEEE Trans. on Wireless Comm., vol. 10, no. 11, pp. 3973-3983.
[33] Zhang, W., Das, S. K., Liu, Y,Security in Wireless Sensor Networks: A Survey,in Y.Xiao (2007),Security in Sensor Networks, Auerbach Pubilication ,pp 237-272.
[34] Kaur Veerpal & Singh Aman(2013), Review of Various Algorithms Used in Hybrid Cryptography International Journal of Computer Science and Network, Volume 2, Issue 6.
[35] Dhillon, J. ,Prasad, K., Kumar, R. and Gill,A(2011),Secure Data in Wireless Sensor Network By Using DES,International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 3.
[36] Kaur, A.(2013),Energy Analysis of Wireless Sensor Networks using RSA and ECC Encryption Method, International Journal of Scientific & Engineering Research, Volume 4, Issue 5, May-2013 2212 ISSN 2229-5518 IJSER .
[37] Zhao, G.,Yang, X.,Zhou, B. and Wei,W.(2010), RSA-based digital image encryption algorithm in wireless sensor networks, 2nd IEEE International Conference on Signal Processing Systems (ICSPS).
[38] Lee, H., Lee, K., and Shin, Y.(2010), Implementation and Performance Analysis of AES-128 CBC algorithm in WSNs, in 12th International Conference on Advanced Communication Technology, pp. 243-248.
[39] Shanyue, B. & Liqing, C.(2012), A new key management protocol for wireless sensor network, " in International Conference on Computer Science Service System (CSSS), pp. 991-994.