Adaptive Data Size Compressed Algorithm to Reduce Energy and Provide Route Security using AOMDV Protocol in WSN

Ajay Kumar
Research Scholar in
Computer Science & Engineering
M.M.U Mullana, Ambala, India

Rohit Vaid, PhD
Assistant Professor in
Department of Computer
Science & Engineering
M.M.U Mullana, Ambala, India

Sandhya Katiyar
Assistant Professor
In Department of
Information Technology
Galgotia's College of
Engineering and Technology,
Greater Noida, India

Shumaila Rizwan
M.Tech student in
Department of Information Technology
Galgotia's College of
Engineering and Technology,
Greater Noida, India

ABSTRACT
In this research paper an algorithm is generated named Adaptive Data Size Compressed Algorithm (ADSCA) in wireless sensor network. This algorithm depends on the binary numbers and the hash function. Binary numbers are using for compress data length or data size with the help of ASCII code and hash function is also used to compress the data size without losing information. After that the electromagnetic waves are used for data transmission from one node to another node. Then it is analyzed that how much minimum energy should be used in data transmission from source to destination through the electromagnetic waves. For the security purpose two techniques are applying, one is RSA algorithm and other is Diffie-Hellman algorithm. The latest routing protocol for sending the information is AOMDV, which is an extension version of AODV protocol. With the help of this routing protocol and security techniques, a secure route and minimum numbers of hop counts are find out from source to destination for sending the information data. At last MATLAB represents the data transmission from source to destination is dynamically showing in GUI (Graphical User Interface). This GUI is created a wireless sensor network, where some sensor nodes are deployed.

Keywords
ADSCA, RSA, WSN, AOMDV protocol, Diffie-Hellman algorithm, Hashing, Binary code, ASCII code, Security, MATLAB.

1. INTRODUCTION
In today's life Wireless Sensor Networks (WSNs) are one of the most important technologies which have been widely used. WSN is used for collecting the information from the environment. WSN consists of a large number of sensor nodes, each sensor node in network are connected by a wireless channels. Each sensor node in wireless sensor network equipped with its own sensors, processor and radio transceiver [1].

WSNs enabled by advance microelectronic mechanical systems (MEMS) and wireless communication technologies, which are tiny, cheap and smart sensors deployed in a physical area and networked through wireless links and the Internet offer unprecedented opportunities for a variety of civilian and military applications, for example, environmental monitoring, battle field surveillance, and industry process control [2]. A wireless sensor node consists of a processor, sensor, communication module powered by a battery. The major issue in WSNs is Power efficiency, because if energy is used efficiently, it increases or extends the network lifetime. During sensing, processing and transmission the energy is consumed by the sensor node. But almost 70-80% of the energy is spent during the data transmission in wireless sensor network. There are many researchers show that for extending the lifetime of sensor nodes may take place by reducing the energy required for transmission. A number of algorithms have been proposed for energy efficient wireless sensor network in literature. WSNs with long lifetime requirements have severe power constraints. Data compression, not many have worked in lossless algorithms for WSNs. Compression algorithms are not only the data storage but simple and application specific also and they required for resource constrained sensor nodes [3].

AOMDV is the extended version of AODV protocol to discover multiple paths between the source and the destination in every route discovery. Multiple paths so computed are surely to be loop-free and disjoint. AOMDV has three novel aspects compared to other on-demand multipath protocols. First, like other protocols AOMDV does not have high inter-nodal coordination overheads (e.g., TORA [9], ROAM [10]). Second, without the use of source routing AOMDV protocol ensures disjointness of alternate routes via distributed computation. Finally, AOMDV protocol computes alternate paths with negligible additional overhead over AODV protocol; AOMDV protocol does this by exploiting already available alternate path routing information as much as possible [4].

2. PROBLEM IDENTIFICATION AND PROPOSED WORK
There are the biggest problem that how can be reduced energy loss for transferring information and security in wireless sensor networks. to overcome this problem an algorithm is

given named adaptive data size compressed algorithm (ADSCA) which works as for alphabets and symbols binary code conversion using ASCII code, and for the data which is in the form of image, audio and video are compressed by using hash function and for data transmission, electromagnetic waves are used which can transfer the data packets or information. Electromagnetic waves energy E is directly proportional to the electromagnetic mass M (data packet length/size) and travels with the speed of light c which is constant. In this figure three main properties have been proposed to give all sensor nodes in WSN.

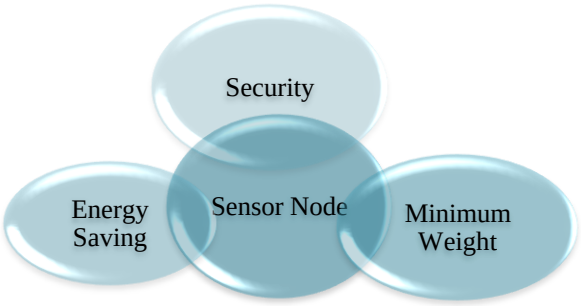

Fig 1: Proposed sensor node property

- *Minimum weight*: For the adaptive environment, it is necessary to reduce the data packet size. These small data packets contain large information i.e. maximum information can be easily transferred.
- *Energy saving*: Minimum energy consumed during data transmission. Since data packets size are small.
- *Security*: Maintain the route security for data packets transmission.

In wireless sensor network (WSN) security is the major concern. Not only the data should be transferred from source to destination securely but also less energy should be consumed by nodes and there must be loss less communication between nodes. The researchers have developed a number of techniques, but when the multiple path routing technique is taken, the researchers are not much succeeded in security and energy efficiency at a same time. So there a solution is given, in which key concept is not being used because in the management of keys, lots of energy is consumed by sensor nodes. A secured routing algorithm is given which provides secured data transfer as well as find attacked node or exposed node also and also take less energy which is called energy efficient. A concept of multi path routing is introduced which is influenced from multipath distance vector routing.

AODV (Ad-hoc on demand distance vector routing protocol) has been widely used protocol in MANET. But AODV and other on demand routing protocol use single route reply. An extension version of AODV called AOMDV which enhances the network performances like packet delivery ratio. Another issue in AODV is sending unicast traffic while AOMDV allows each node in the network to send out multicast data packets.

Now to provide security, a Diffie-Hellman and RSA algorithms are applied separately and then compared their performance on the basis of timing.

Here is a proposed network below; where MATLAB represents the data transmission dynamically showing with the help of Graphical User Interface. This GUI is produced a wireless sensor network, where a few sensor nodes are deployed.

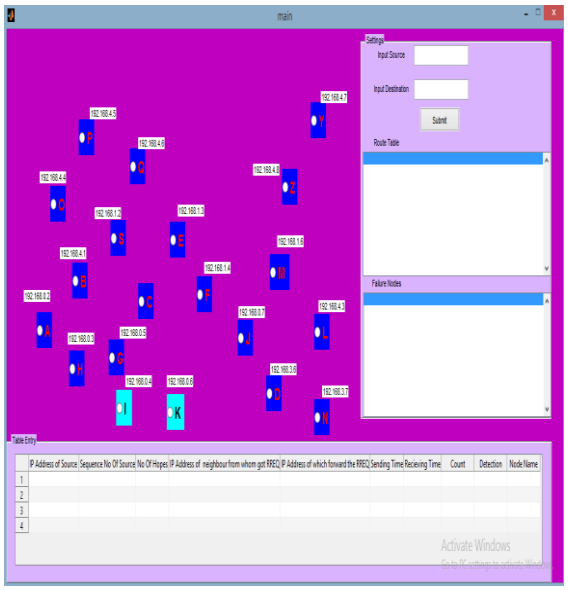

Fig 2: Proposed Network

3. ADAPTIVE DATA SIZE COMPRESSED ALGORITHM (ADSCA)

Now a day's there are many types of algorithms are used to minimize the data. In this paper the data is compressing by binary conversion and hashing. There are different types of data in the form of alphabets, numbers, symbols, image, audio and video. These types of data transfer one node to other node from source to destination. We have generated the adaptive data size compressed algorithm which compress the message data without losing information and reduce the message size or minimize the energy with the help of electromagnetic waves formula. The electromagnetic waves flow with the speed of light and the energy is directly proportional to the mass. The data which is in the form of text is converted into the binary values which is only in terms of (0, 1) with the help of American Standard Code for Information Interchange (ASCII) and divided into the 8 byte sets for compression and the data which is in the form of image, audio and video are compressed with hashing H(M). Hashing is also compressed data without losing information. And after that the compressed data energy can be calculated with the help of electromagnetic wave formula.

$$E_{em} = \frac{3}{4} m_{em} c^2$$

Where,

- c^2 is the speed of light which value is constant that is $3x10^8$m/s.
- m_{em} is the value of electromagnetic mass/weight, which is equivalent to the data base size in bytes.
- E_{em} is the value of electromagnetic energy.

The adaptive data size compressed algorithm which minimizes the data size and reduce energy because of the

electromagnetic waves energy is directly proportional to the mass of data. The algorithm is as follows:

Step1: Initialize the message (M).

Step2: Calculate the original message (M) energy using electromagnetic waves formula,

$E_{em} = \frac{3}{4} m_{em} c^2$

Step3: If the messages in the form of text then convert it into the binary values (0, 1) using ASCII codes.

Step4: Then divided into the 8 byte sets of whole message.

1 bit = 8 byte

Step5: Safely compressed all the data without losing information.

Step6: if

Message in the form of image, audio and video then apply hash function to minimize this message data.

H(M)

else

Repeat step 3, 4, 5.

Step7: Now repeat step 2 to calculate the energy of new data weight.

E_1=, where m_1 is new string length.

Step8: Compare the both energy to find out the average energy.

$\Delta E = E_{em} - E_1$

Step9: End of the algorithm steps.

The flowchart is giving by the steps of the ADSCA algorithm as shown in the figure3.

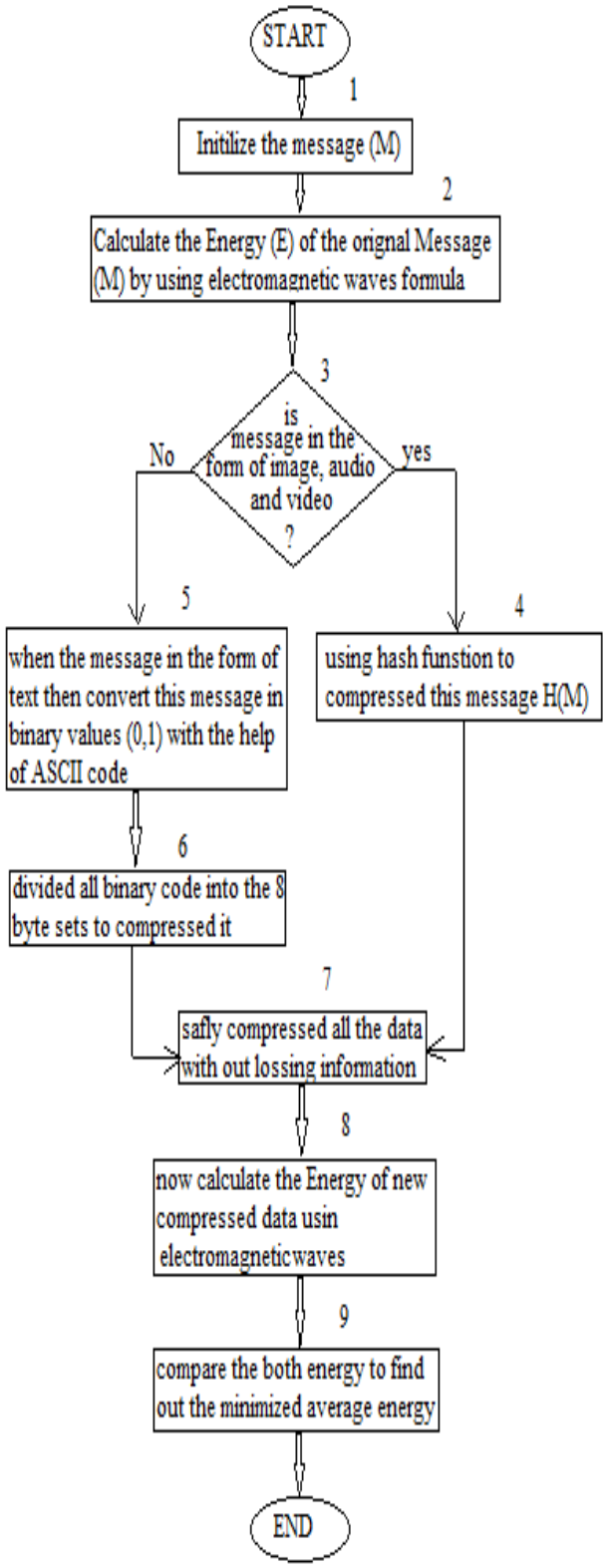

Fig 3: flowchart of ADSCA algorithm

ASCII code and binary code tables are given below.

Table 1. The binary numbers of ASCII characters

Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code	Character	Binary Code
A	01000001	Q	01010001	g	01100111	w	01110111	-	00101101
B	01000010	R	01010010	h	01101000	x	01111000	.	00101110
C	01000011	S	01010011	i	01101001	y	01111001	/	00101111
D	01000100	T	01010100	j	01101010	z	01111010	0	00110000
E	01000101	U	01010101	k	01101011	!	00100001	1	00110001
F	01000110	V	01010110	l	01101100	"	00100010	2	00110010
G	01000111	W	01010111	m	01101101	#	00100011	3	00110011
H	01001000	X	01011000	n	01101110	$	00100100	4	00110100
I	01001001	Y	01011001	o	01101111	%	00100101	5	00110101
J	01001010	Z	01011010	p	01110000	&	00100110	6	00110110
K	01001011	a	01100001	q	01110001	'	00100111	7	00110111
L	01001100	b	01100010	r	01110010	(	00101000	8	00111000
M	01001101	c	01100011	s	01110011	)	00101001	9	00111001
N	01001110	d	01100100	t	01110100	*	00101010	?	00111111
O	01001111	e	01100101	u	01110101	+	00101011	@	01000000
P	01010000	f	01100110	v	01110110	,	00101100	_	01011111

Table 2. Alphabets position numbers of ASCII code

A	**65**	**N**	**78**	**A**	**97**	**n**	**110**
B	**66**	**O**	**79**	**B**	**98**	**o**	**111**
C	**67**	**P**	**80**	**C**	**99**	**p**	**112**
D	**68**	**Q**	**81**	**D**	**100**	**q**	**113**
E	**69**	**R**	**82**	**E**	**101**	**r**	**114**
F	**70**	**S**	**83**	**F**	**102**	**s**	**115**
G	**71**	**T**	**84**	**G**	**103**	**t**	**116**
H	**72**	**U**	**85**	**H**	**104**	**u**	**117**
I	**73**	**V**	**86**	**i**	**105**	**v**	**118**
J	**74**	**W**	**87**	**j**	**106**	**w**	**119**
K	**75**	**X**	**88**	**k**	**107**	**x**	**120**
L	**76**	**Y**	**89**	**l**	**108**	**y**	**121**
M	**77**	**Z**	**90**	**m**	**109**	**z**	**122**

4. AODV (AD – HOC ON DEMAND DISTANCE VECTOR) ROUTING PROTOCOL

Routing protocols of WSN can be classified as reactive and proactive. In reactive routing protocols the routes are formed only when source wants to send data to destination while proactive routing protocols are table driven. AODV routing protocol is one of the most well known reactive routing protocols of wireless sensor networks. Being a reactive routing protocol AODV uses traditional routing tables, one entry per destination and destination sequence numbers (DSN) are used to verify whether routing information is up-to-date and to prevent routing loops. This will highly increase the efficiency of routing processes. AODV consist of two routing phases such as discovery and maintenance [5].

AOMDV (Ad-Hoc On-Demand Multipath Distance Vector Routing Protocol) extends the AODV protocol to determine multiple paths between the source and the destination in every route. Multiple paths so calculated are surely to be loop free and link disjoints. AOMDV also finds routes on-demand using a route discovery procedure. A new class of on-demand routing protocols for mobile ad-hoc networks have been created with the aim of minimizing the routing overhead. The key characteristics of an on-demand protocol are the source initiated route discovery process. The on-demand protocols, multipath protocols have a comparatively higher ability to overcome the route discovery frequency than single path protocols. On-demand multipath protocols find out multiple paths between the source and the destination in a single route discovery. So, a new route discovery is required only when all these paths fail. Routing done by using the AOMDV routing protocol. AOMDV depends on as much on the routing information already available in the known AODV protocol, thus limiting the overhead exes in discovering multiple paths. It does not want any special control packets. Further RREPs and RERRs for multipath discovery and maintenance along with a few extra fields in routing control packets (i.e. RREQs, RREPs and RERRs) compose the only additional overhead in AOMDV relative to AODV [6].

5. RSA AND DIFFIE-HELLMAN ALGORITHMS FOR SECURITY

A cryptographic algorithm is mostly used RSA. By using this algorithm, the data packets are transferred through dynamic routing by time to time key value change safely.RSA implements two main ideas: Public- key encryption and Private-key decryption. In RSA, encryption keys are public, while the decryption keys are not. The person with the right decryption key can decode an encrypted message. Everyone has their own encryption and decryption keys [7].

The Diffie-Hellman key agreement protocol (1976) was the first practical method for establishing a shared secret over an unsecured communication channel.

The Diffie-Hellman algorithm with example is as follows:

- A and B agree on a prime number (p=23) and a base (g=5).
- A chooses a top secret number (a=6) and sends B.g^a mod p = 5^6 mod 23 = 8
- B chooses a top secret number (b=15) and sends A.g^b mod p = 5^{15} mod 23 = 19
- A computes $(g^b \bmod p)^a \bmod p = 2$
- B computes $(g^a \bmod p)^b \bmod p = 2$
- After that 2 is the shred top secret.

Clearly, much larger values of A, B and p are needed. An eavesdropper cannot discover this value.

The strong cryptography algorithm, such as RSA algorithm is proposed to be used in WSN_s even there are lots of constrains including high time complexity and power consumption. For RSA encryption in the RSA coding algorithm four processes needed i.e. In brief; the RSA algorithm is following [8]:

1. Creating a public key
2. Creating a private key
3. Encode the message
4. Decode the message

To create public key K_P:

a. Pick two dissimilar primes P and Q

b. Allocate x=(P-1)(Q-1)

c. Prefer E comparative primes to x, which have to suit a situation for K_s.

d. Allocate N=P*Q

e. K_P is N concatenated with E.

To encode basic text m by:

a. Suppose m is a numeric

b. Compute $c= m^E \bmod N$.

To decode c reverse to m

a. Compute $m= c^D \bmod N$.

These security algorithms are applied to the proposed model for finding a secure route and by using AOMDV protocol hop-by-hop process a shortest route find out from source node to destination node. With the help of ADSCA, the energy consumptions can be minimized for data forwarding.

6. IMPLEMENTATION IN MATLAB FOR DATA TRAVERSING USING GUI

There are some figures in MATLAB'S GUI (graphic user interface) are showing the transmission of message information's.

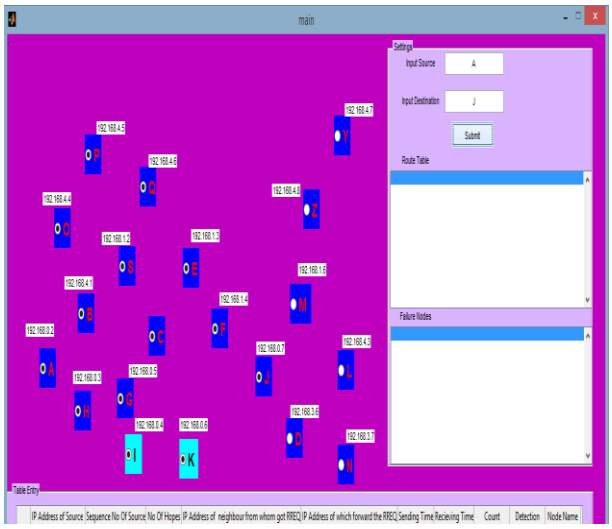

Fig 4: Traverse all nodes from A to J

In this figure there are some sensor nodes designed in a wireless sensor network. Here we assume that "A" is a source node which has some information sends to the destination node "J" through all nearest nodes by AOMDV routing protocol which is using the hop-by-hop process.

1. A→B→S→C→F→J
2. A→B→O→P→Q→E→F→J
3. A→H→G→I→K→J

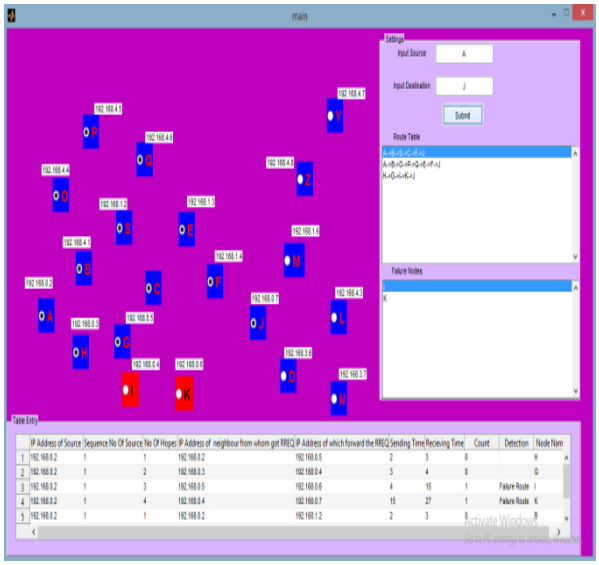

Fig 5: Showing failure nodes from A to J

In this figure the node I and K are representing the failure route.

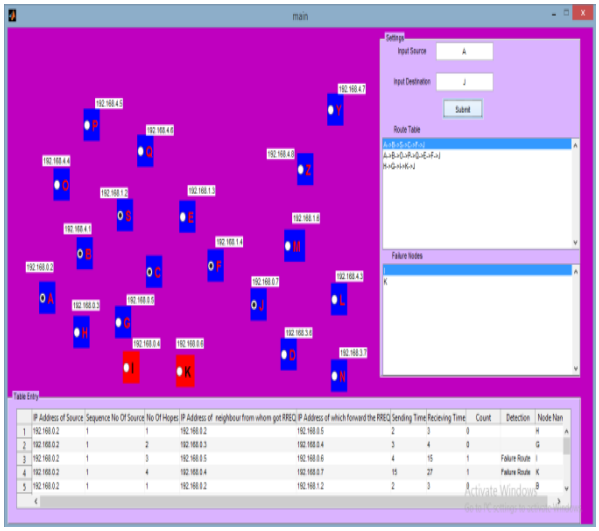

Fig 6: showing a clear route from A to J

Now in this figure shows a secure route which is, (A→B→S→C→F→J) a secure route without any failure node. Then data packets are safely sent from source "A" to destination "J".

7. RESULTS AND ANALYSIS

It is very effective to use electromagnetic waves for data transmission. Since the electromagnetic waves are travelled with the speed of light and the mass of data packets are directly proportional to the energy which is consumed during data transmission or for forwarding the data from source node to destination node, by using the electromagnetic waves formula that is:

$E_{em} = \frac{3}{4} m_{em} c^2$ (where, c is constant)

The given graph is showing the performance of mass and energy according to this formula.

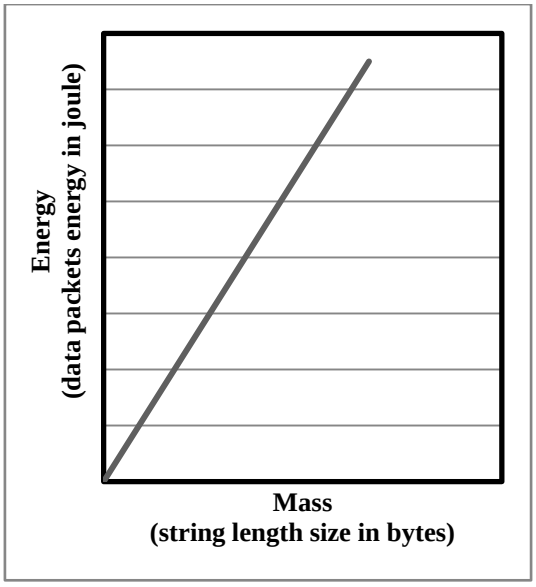

Fig 7: Mass V_S Energy graph

Now according to the formula it is analyzed that the reduction of mass and energy is directly proportional to each other as mass reduces, energy also reduces and if mass increases, energy also increases and by using ADSCA algorithm it is possible to reduce the message mass/data size without losing information. The analysis graphs are given below.

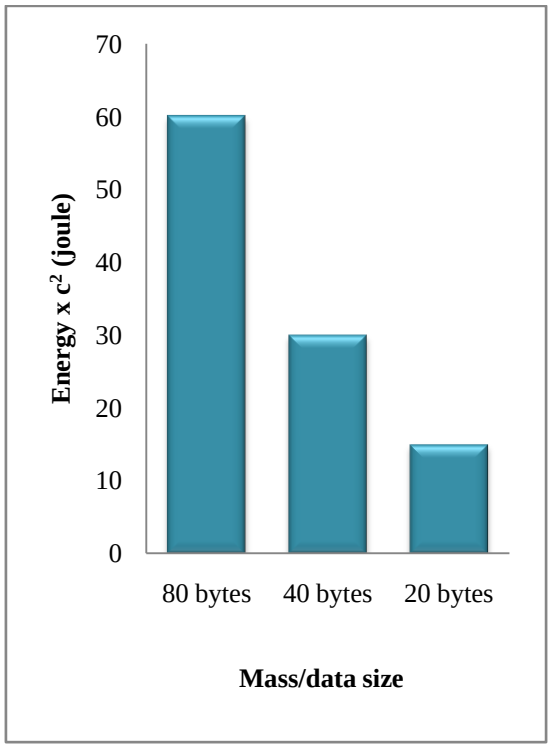

Fig 8: graph when falling the mass and falling the energy

According to the formula suppose the value of mass is,

m_1 = 80 bytes, m_2 = 40 bytes and last m_3 = 20 bytes then calculate the energy in terms of c is:

$E_1 = (3/4) \times 80 \times c2 = 60\ c^2$ J

$E_2 = (3/4) \times 40 \times c^2 = 30\ c^2$ J

$E_3 = (3/4) \times 20 \times c^2 = 15\ c^2$ J

Where, c is the constant and value of $c = 3 \times 10^8$ m/s which flow is equal to the speed of light.

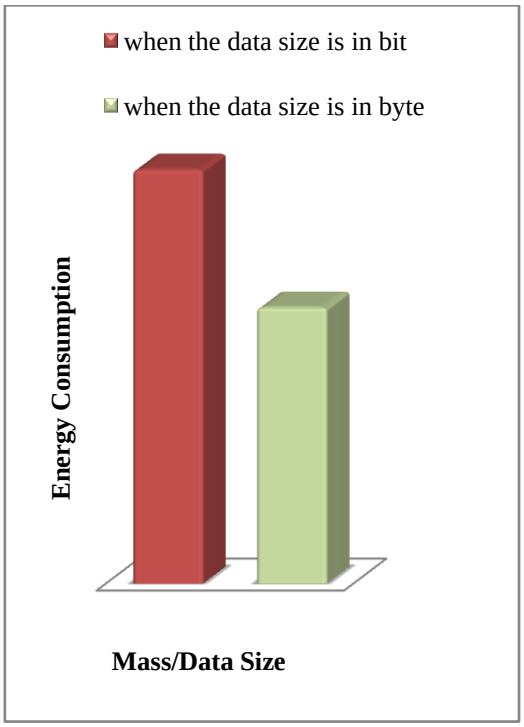

Fig 9: Performance Graph of Energy Consumption

After applying the proposed algorithm the energy consumption is decreased as shown in the figure9.

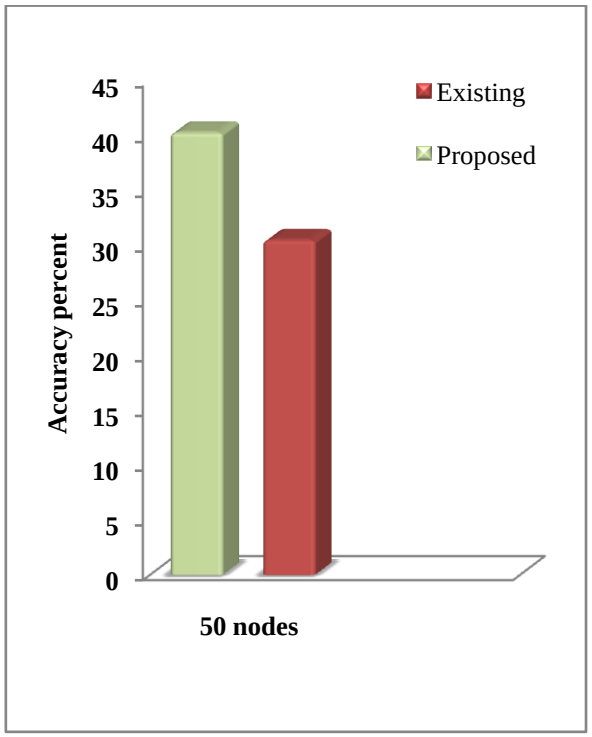

Fig 10: Accuracy Performance Graph of Security

This graph shows clearly the accuracy of node security. The performance of given concept for security is better than earlier existing concepts. So by using given algorithm with security the accuracy is increased and information is protected throughout the transmission.

8. CONCLUSION AND FUTURE SCOPE

In this research paper ADSCA algorithm is generated in WSN which is used to solve the problem of more energy consumption during data transmission and also provided a secure data transmission throughout the network. This algorithms works as for alphabets and symbols binary code conversion using ASCII code, and for the data which is in the form of image, audio and video are compressed by using hash function and for data transmission, electromagnetic waves are used which can transfer the data packets or information. Electromagnetic waves energy E is directly proportional to the electromagnetic mass M (data packet length/size) and travels with the speed of light c which is constant. By using ADSCA algorithm the energy consumption will be reduced and more secured data will be transferred from source to destination node. To minimize the energy consumption, electromagnetic waves are used with the speed of light while transmitting the data in the network. Next to provide the security, cryptographic algorithms RSA and Diffie-Hellman are used with AOMDV protocol.

In future this research work can be extended by taking some hybrid protocol which are commonly zone base protocol and can be implemented with both reactive as well as proactive routing protocols and data can be compressed by bit rate reduction and JPEG image compression techniques which might be applicable on textual and audio/video data at a time.

9. REFERENCES

[1] et al. L.Sujihelen, C.JayaKumar, "Authentication in wireless sensor network based on Virtual Certificate Authority", International Conference on circuits, power and computing technologies, 2013 IEEE.

[2] et al. Chugh and Singh, A Real-Time MATLAB based GUI for node placement and a shortest- path alternate route path algorithm in Wireless Sensor Networks , "International Journal for Science and Emerging Technologies with Latest Trends"(2013)ISSN No. (Print): 2277-8136.

[3] "Power Efficient Adaptive Compression Technique for Wireless Sensor Networks", et al. S. Selvarani,S. Selvaraju, P. Yasodha Devi, S. Kalaivani, M. Vasanth, M.Kannan, IOSR Journal of VLSI and Signal Processing (IOSR-JVSP) Volume 3, Issue 4 (Nov. – Dec. 2013).

[4] et al. Mahesh K. Marina and Samir R. Das, "Ad hoc on-demand multipath distance vector routing", wireless communications and mobile computing2006; 6:969–988.

[5] et al. P.Samundiswary and P.Dananjayan, "Performance Analysis of Trust Based AODV for Wireless Sensor Networks", International Journal of Computer Applications (0975 – 8887) Volume 4– No.12, August 2010.

[6] et al. Vishnupriya E, Prof. T. Jayasankar, "Performance Analysis Of Optimum Routing Protocols In Wireless Sensor Networks", IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 2 Issue 2, February 2015, ISSN 2348 – 7968.

[7] "Data Aggregation Using RSA Key Management Technique in Wireless Sensor Networks ", C. Krishnan, Mrs. G.Malathy, IJIRSET, Volume 3, and Special Issue 1, February 2014, ISSN (Print) : 2347 – 6710.

[8] et al. Abdullah Said Alkalbani, Teddy Mantoro, Abu Osman Md Tap, "Comparison between RSA Hardware and Software Implementation for WSNs Security Schemes", Proceeding 3rd International Conference on ICT4M 2010.

[9] Park VD, Corson MS. A highly adaptive distributed routing algorithm for mobile wireless networks. In Proceedings of IEEE Info.com, 1997.

[10] Raju J, Garcia-Luna-Aceves JJ. A new approach to on-demand loop-free multipath routing. In Proceedings of Int'l Conference on Computers Communication and Networks (IC3N), 1999.