Secure user Authentication and File Transfer in Wireless Sensor Network using Improved AES Algorithm

Ishu Gupta
Research Scholar
Punjab Technical University

Dr Harsh SadaWarti
Professor
C.T. University Jalandhar

Dr S.N Panda
Professor
Chitkara University,Rajpura

Jatin Gupta
Assisant Professor
Chitkara University,Rajpura

***Abstract*—The WSN technology is a highly efficient and effective way of gathering highly sensitive information and is often deployed in mission-critical applications, which makes the security of its data transmission of vital significance. However, the previous research paper failed to distinguish the role of centralized server for it being the main controller of the entire network. The decision of nodes communicating with each other in the previous research paper was based on the information received from the adjacent node. However, the proposed research paper will take into account the centralized server to develop a new technique to prevent the black node from joining the wireless sensor network. Key distribution technique along with the implementation of improved AES algorithm double key encryption will play an important role in transferring the data between authorized nodes securely and preventing unauthorized user from accessing it.**

Keywords—Wireless sensor networks (WSN); centralized server; black node; encryption; security; key distribution technique

I. INTRODUCTION

The wireless sensor networks (WSN) are specialized transducers with spatially dispersed and dedicated autonomous sensor nodes for identifying, monitoring and recording the physical and environmental conditions at different locations. Of the most commonly monitored physical parameters include temperature, pressure, light, direction of wind and its speed, intensity of illumination, vibration and sound, chemical concentration in water, air, pollutant level, humidity, vital body functions and so on.

WSN is a revolutionary technology that comprises of several sensor nodes that are small in size, light in weigh and easily portable. These sensor nodes are laced with a radio transceiver, a microcontroller and a battery, which can either be embedded in it or located externally as an energy resource. The function of the radio transceiver is to connect the sensor nodes or neighbor nodes with an external link while the microcontroller is an electronic circuit that plays a significant role to interface the sensor nodes thereby forming a complete circuit to effectively process, store, receive and send data to the base station.

This hi-end information gathering technology was originated as an initiative of keeping surveillance checks in the wars or battlefields. With its great potential applications, today, it is widely and effectively deployed in wide-mission vital military operations, various industries monitoring the health of machineries, agriculture and commercial domains for monitoring and controlling various other applications. As the WSN deals in highly sensitive information, its processing, gathering and transmittance, therefore, security in this spatially dispersed nodal network is of crucial concern. This kind of highly sensitive data, which can be related to a patient for its medical background data, military operations related strategies or highly confidential mission data, data related to earthquake, or other such environment calamity and much more must be dispersed or transmitted in an encrypted format. As any leakage or misuse of this critical information or data can create serious issues and impact an individual or the entire nation badly, thus, it becomes of paramount importance to secure the data of the sensory nodal network by deploying effective and efficient network security techniques.

Wireless sensor networks are one of the most intriguing yet most challenging technologies of the current times due to its built-in complexity. The sensor nodes of WSN work under extreme resource constraints as the energy resource usually comprises of an embedded device with limited supply to transmit data in a highly unspecified environment. Being a wireless mode of network, the chances of data packets getting damaged due to an unwanted error, or conflict amongst the nodes or over congestion is very high. As the entire security mechanism of the network depends upon the cryptographic key distribution and reporting of critical events, the unreliable mode of communication amongst the sensor nodes poses grave threat to the security of the network. Additionally, sending and receiving secure data in highly callous conditions is not an easy task as the sensor nodes have the tendency to closely interact with their physical environment to process and blend data and

create novel information that must be transmitted to the end-station. However, these uncontrolled operations in unattended environment may create accidental node failure.

The security of Wireless Sensor Network (WSN) is under grave threat due to the attacks on the sensor nodes, which are often categorized as goal-oriented attacks, performer-oriented attacks and layer-oriented attacks. Goal-oriented attacks are mainly against the data confidentiality wherein an attacker passively monitors the traffic, analyzes it for imperceptibly encrypted sensitive information and then gains authentication information to pass through the network. This type of attack is called passive attack which results in the revelation of sensitive information to the attacker without any knowledge at the user's part. However, in the active attack, the attacker actively assesses the entire network to gain control over it. The best and most common ways of active attack includes data modification, spoofing, sinkhole, flooding, jamming the network, warm hole, black hole, fabrication, lack of co-ordination, node subversion, false nodes, selective forwarding and so on. While in performer-oriented attacks, the attacks are either internal or external. Internal attackers are the trickiest ones as they are not only the legitimate node of the original network but also have direct access to all the sensitive network information. The internal attacks include modification, misrouting, eavesdropping and packet dropping attacks that leads to suppression of critical information reaching the base station, thereby degrading the network performance. On the other hand, external attackers are known for eavesdropping on transmittance of data along with injecting fake data in the network to exhaust energy resource, which will lead to denial of services. Another attack on WSN are related to its layered architecture, which makes it susceptible to node capturing, jamming of radio signals, violating redefined protocols, inducing collisions by disrupting a packet, depletion of energy due to recurring retransmission and new connection request to avert the sensor nodes from communicating effectively.

As of now, trust management system is considered to be the most effective and efficient way of dealing with the attacks on the sensor nodes of a wireless network. Trust factor is a very important and useful concept for WSN for detecting the attacks on the sensor nodes and accordingly support in the process of decision making. The concept has grown its relevance with the rising use of internet transaction and e-commerce. Considering trust as an important parameter in the relationship between two nodes, it becomes quite easy to identify the innate qualms in their co-operation process.

This concept of trust has been originated from the sociological and psychological environment, which makes it an essential element in any kind of network, be it social or computer related. Generally, a trust management system is broadly classified into two types: credential based trust management system and behavior based trust management system.

II. Literature Survey

A lot of researchers have worked in this field to provide fool proof algorithms to avoid the security breaches of the wireless sensor network. The unwanted and unnecessary challenges associated with the sensory nodes of wireless network makes it intricate to employ the proposed security approaches of the researchers in the past. However, careful and diligent understanding of these challenges along with the susceptible attacks on the sensor nodes can definitely aid the researchers in proposing or presenting an algorithm that would work efficiently and effectively in handling the security breaches and enhancing the security in the wireless sensor network.

Geetha D. Devanagavi et al. [1] in their research proposed an agent based Secured Routing using Trusted neighbors (ASERT) in WSN. The proposed technique ensures high security by selecting the trustworthy neighbors and formulating the secured routes in the network using probability based trust model and MAC model. In this task, software agents play a pivotal role. The entire process of identifying trusted neighbors is divided into two phases: the first phase involves agents visiting all the neighbors one by one and determining their probability using trust model and in the second phase, MAC model is used to ensure the trusted neighbors.

Monia, Sukhchandan Randhawa and Sushma Jain [2] in their research study proposed an improved algorithm in which the cluster heads are chosen based on the received signal. Calculation of trust values and malicious node detection is done by considering the packet forwarding factor. The proposed technique also takes into account the consistency of clusters and lifetime of the network.

Mukesh Kumar and Kamlesh Dutta [3] put forth a literature survey to elaborately discuss concerns that can cause the security breach in data aggregation. It vividly describes the basics of aggregating the data in WSN in a secured manner, important factors to be taken into account for classifying the secured data aggregation techniques for WSN, key aspects of the existing data aggregation techniques and a crisp comparison of these techniques based on parameters like aggregation function, cryptographic techniques used in WSNs etc.

Vinod Kumar Verma, Surinder Singh, N. P. Pathak [4] intended to investigate the repercussions of static, dynamic and oscillating modes by performing prevalent analysis of wireless networks. The parameters like accuracy, path length and energy consumption are taken into account to examine the impact of different WSN modes on the deployed trust and reputation models: Bio-inspired trust and reputation, Eigen trust, peer trust, power trust and linguistic fuzzy trust and reputation.

Weidong Fang, Chuanlei Zhang, Zhidong Shi, Qing Zhao, and Lianhai Shan [5] proposed a beta based trust and reputation evaluation method which employs the beta distribution to determine the credibility of nodes distribution. The calculated trust values are utilized to choose the relay nodes and counteract the internal attacks. Intensive experimental results exhibit higher information security and maximize shield against various types of internal attacks from malicious nodes.

X. Anita, M. A. Bhagyaveni, J. Martin Leo Manickam [6] suggested a minimal overhead trust management scheme in terms of memory and energy consumption. Instead of deriving

the trust values of the neighboring nodes haphazardly, it employs a novel trust detector that monitors and alarms the nodes whose trust falls below a minimum threshold. This warning motivates the sensor nodes to improve its trust relationship with other nodes by analyzing and rectifying its packet forwarding behavior.

Yun Liu, Chen-xu Liu, Qing-An Zeng [7] formulated an improved trust management system derived from the trust model in the iRTEDA protocol which is utilized to attain the secured data aggregation pertaining to the nature of relationship between the nodes in the network. The proposed trust model intends to efficiently utilize the second –hand information from the neighboring nodes and to attain the maximum level of security for aggregating the data and evaluating the trust and reputation of the nodes.

Yannis Stelios, Nikos Papayanoulas, Panagiotis Trakadas, Sotiris Maniatis, Helen C. Leligou, and Theodore Zahariadis [8] proposed a novel trust and reputation system which detects a wide range of security threats. The proposed model exhibits effective estimation of malicious nodes and sustains the network connectivity even when the malicious nodes comprise majority of the network. It also incorporates the energy awareness in the network.

III. Problem Statement

The existing research study has a big drawback in terms of not explaining the role of centralized server in checking the trust value of the nodes. Despite centralized server being the main controller of the entire network, the decision of nodes communicating with each other is based on the information received from the adjacent node. In such cases, presence of a black node in the network can cause severe damage to the network. Therefore, a black node can pose a big threat if the centralized network fails to detect its entry in the network, joining and connecting with other nodes as black node is known for sending wrong information to other nodes, thereby affecting the trust value of the target node as a whole.

With this drawback in mind, the main emphasis of the proposed research study is to check the trust factor of node from the centralized server i.e. the cluster head (CH) that controls the whole network to prevent the problem of black node. Additionally, we have set a number of rules to prevent the black node enter and disrupt the wireless Sensor Network and its functioning, which are discussed in the proposed work.

IV. Proposed Work

1) Registration Phase: In registration phase, server will give Big Integer unique key, an ID to user.

2) Login Phase: For fresh node, there will be two phases to join the network:

a) Authentication phase, wherein the authentication phase server will check the following parameters:

- mac Address,
- username,
- password, and
- unique key.

If all these parameters are matched, only then authentication will be completed for the server to send an encrypted message to the Client.

b) Authorization Phase: In this, a user will decrypt the message received by server by using his / her designated key and send it to the server for matching. If the decrypted message gets matched with the sending message, only then the authorization phase will be completed for the user to log in.

3) File Sharing: When user wants to share the file, firstly key agreement phase will be placed which will be done by using IBE algorithm.

Algorithm steps:

Firstly, user requests to the server for receiver's ID, public key and a number.

a) User will encrypt the message using receiver's ID, public key, and a number that he gets from the server.

b) Receiver will decrypt this challenge using its private key, number, user ID that he gets from the server.

If receiver decrypted message matches with the sender message, only then file sharing is possible between them.

A. Encryption

On the server, file will be encrypted, using RSA with homomorphic + AES algorithm;

Steps:

1) Apply Homomorphic with RSA algorithm: The homomorphic property is meant to preserve the multiplication.

C(x1) â‹…C(x2) = (xe1modm)â‹…(xe2modm)

2) Now using encrypted key, the AES algorithm firstly enables the server to select a master key for the particular user and apply RSA Homomorphic on it as and it returns digital signature which is used as key (1244812334565456)

Key (1244812334565456) in hexadecimal is→ 31 32 34 34 38 31 32 33 33 34 35 36 35 34 35 36

Now suppose, we have plain text to be encrypted as: "Wireless sensor"

Change it to Hexadecimal code: 57 69 72 65 6c 65 73 73 20 20 73 65 6e 73 6f 72

Perform X-OR operation on it with key as:

31 38 33 35		
32 31 34 34		
34 32 35 35	X-OR with	
34 33 36 36		
57 6c 20 6e		
69 65 20 73		
72 73 73 6f		
65 73 65 72		

Result:

Suppose it returns as -

54 77 6F 20 4F 6E 65 20 4E 69 6E 65 20 54 77 6F

Pass this cipher text as plain text into AES as - Improved AES:

Key will be generated by main server.

1) Add Round key

In this process, X-OR operation is performed between round key and state. In Aes algorithm the total rounds are 10 but in our Improved Aes algorithm we have reduced 2 rounds to generate cipher text. Round key is generated from the cipher key by using the key expansion process.

AES example - The first round key:

- Round 0: 54 68 61 74 73 20 GD 79 20 4B 75 6E 67 20 46 75
- Round 1: E2 32 FC Fl 91 12 91 88 B1 59 E4 E6 D6 79 A2 93

2) Add Round key

- State Matrix

54 4F 4E 20
77 6E 69 54
6F 65 6E 77
20 20 65 GF

Round 0 Matrix:

54 73 20 67
68 20 4B 20
61 6D 75 46
74 79 GE 75

Perform X-OR operation on state matrix and round 0 matrix.

New Matrix:

00 3C GE 47
1F 4E 22 74
OE 08 1B 31
54 59 OB 1A

Here, we will apply ADD ROUND KEY to this resulted matrix, using digital signature provided by RSA Homomorphic as:

Digital Signature key is→ "1234123412341234";

This key is in hexadecimal is:

57 A1 50 A1 70 80 A0 60 F0 30 AB D1 FF F1 5E F2

00 3C GE 47		
1F 4E 22 74	X-OR with	
OE 08 1B 31		
54 59 OB 1A		
57 70 F0 FF		
A1 80 30 F1		
50 A0 AB 5E		
A1 60 D1 F2		

Suppose Results as:

00 3C GE 47
1F 4E 22 74
OE 08 1B 31
54 59 OB 1A

3) Substitution Bytes

- Current State Matrix:

00 3C 6E 47
1F 4E 22 74
OE 08 1B 31
54 59 OB lA

Firstly, we will change this matrix into 1*4 orders so that we can reduce substitution time as following:

	COL 1	COL 2	COL 3	COL4
		COL 2	COL 3	COL 4
ROW1 →	00 ↓ 1F 0E 54	3C 4E ↓ 08 59	6E 22 ↓ 1B 0B	↓ 47 74 31 1A

In order to increase the throughput, 4 rows are merged into 1 row.

Substitute each entry of current state matrix column wise and find the entries into S-box as following:

a) As 00 1F 0E 54, firstly it will be ordered in the ascending manner 00 0E 1F 54

b) For Example, take 1F to find the entries into S-Box. In 1st row and Fth column, the next entry loop will start from 1 onward, suppose now next value is 54, so loop will start from 1 instead of searching from 0th location.

- Substitute each entry (byte) of current state matrix by corresponding entry in AES S-Box. This leads to new State Matrix:

$$\begin{pmatrix} 63\ EB\ 9F\ AO \\ CO\ 2F\ 93\ 92 \\ AB\ 30\ AF\ C7 \\ 20\ CB\ 2B\ A2 \end{pmatrix}$$

4) Shift Rows

It is an operation that is applied to each row of the matrix state where the first row remains unchanged and the second, third and fourth rows are cyclically shifted on (K-1) basis.

Here k represents the order of the row.

5) Mix Columns

During the mix columns process, each column of the state array is considered as a polynomial. Multiplication using a predefined Matrix is carried out and output is obtained.

The binary calculation based method is used in conventional mix column transformation. The mix columns transformation operates on the state column-by-column. The multiplication method used in mix column transformation.

6) Download File

For downloading a file, user sends request to the server and if user is authenticated, then the server send all the file data to the user.

B. Decryption

At the time of decrypting a file, the request goes to the server and if user is authenticated then server send the encrypted key to the user to decrypt the message by using the following algorithm steps:

1) First select the file to be decrypted.
2) Use the key for decrypting the file.
3) Select the cipher mode for decryption.
4) Now decrypt the final result with the help of AES algorithm.
5) Get the file content into Bytes.
6) Decode this bytes using Base 64 Decoder.

V. Results and Discussion

The energy consumption is represented in Table I and Fig. 1, where with higher nodes consumption is increasing.

TABLE I. Energy Consumption

No. of nodes	Existing	Proposed
10	.008	.006
50	3	2
100	5	4
150	6	7
200	7	8
500	12	15
1000	32	38

Formula: Energy consumption= Load * time

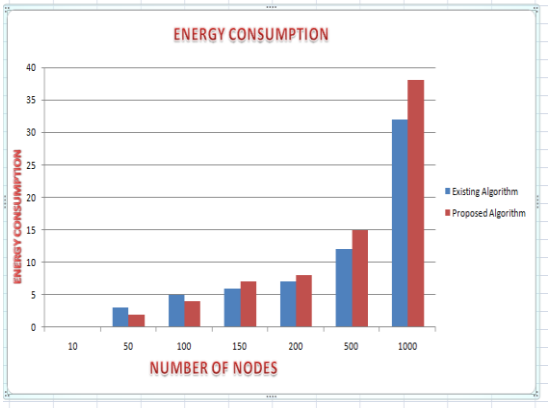

Fig. 1. Energy consumption.

TABLE II. Aggregating Energy

No. of nodes	Existing	Proposed
50	45	50
100	45.80	52
300	46	54.5
500	53	58.5
1000	60	65

Formula: Aggregation accuracy = (Average value of successful transaction/ Total no. of nodes)*100

The aggregating accuracy is represented in Table II and Fig. 2, where the aggregating accuracy for our proposed algorithm is quite better than existing.

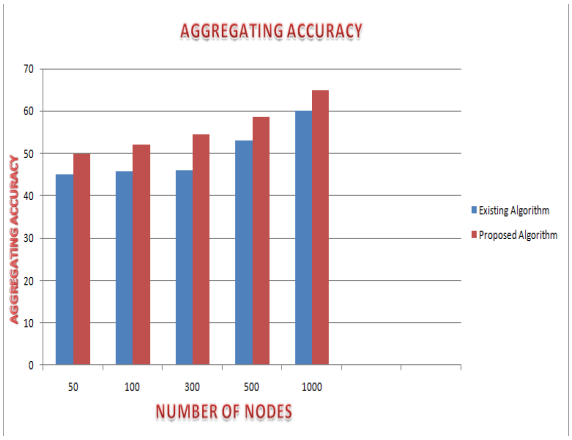

Fig. 2. Aggregating accuracy.

TABLE III. TRUST VALUE

No. of nodes	Existing	Proposed
50	0.5	0.5
100	0.68	0.70
300	0.70	0.72
500	0.75	0.78
1000	0.82	0.87

Formula: Trust value = No of successful transaction of active nodes / Total number of active nodes

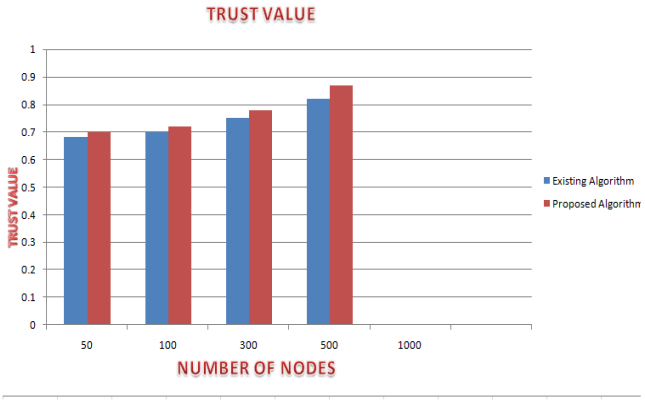

Fig. 3. Trust value of nodes.

The trust value of nodes is given in Table III and in Fig. 3, where the trust value is slightly better for higher number of nodes. The trust is one of the most important parameter of evaluating the routing performance.

TABLE IV. COMPROMISED VALUE

No. of nodes	Existing	Proposed
50	0.5	0.5
100	0.47	0.46
300	0.30	0.28
500	0.29	0.25
1000	0.18	0.15

Formula: Compromised value = 1- No. of successful transaction of every node

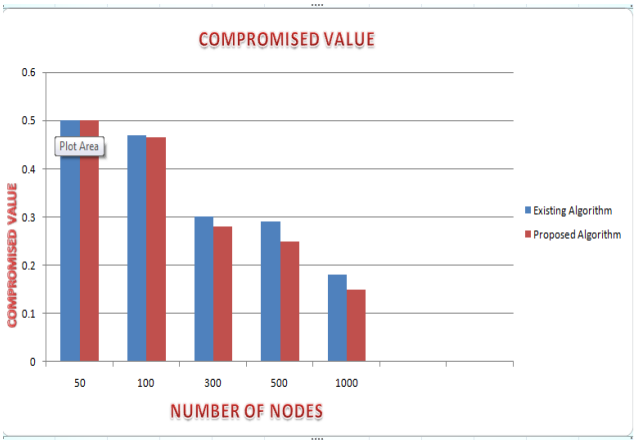

Fig. 4. Compromised value of nodes.

The value of compromised nodes is shown in Table IV and Fig. 4, the compromised nodes are lesser for our proposed algorithm.

VI. CONCLUSION AND FUTURE SCOPE

In our research work, we have developed a new technique to prevent the black node from joining the wireless sensor network. For this, we used key distribution technique along with the implementation of improved AES algorithm double key encryption to not only transfer the data between authorized nodes securely but also prevent unauthorized user from accessing it. Our results regarding trust value, energy consumption, and compromised nodes are enhanced as compared to the previous approaches. However, the only drawback with our research is that if by any chance a black node gets to enter the WSN, then it can easily receive the digital key from the main server and decrypt the data. Therefore, more research needs to be done in this particular area in the future.

REFERENCES

[1] Geetha D. Devanagavi, N. Nalini, Rajashekhar C. Biradar "Trusted Neighbors Based Secured Routing Scheme in Wireless Sensor Networks Using Agents". DOI 10.1007/s11277-014-1704-4. © Springer Science+Business Media New York 2014.

[2] Monia, Sukhchandan Randhawa and Sushma Jain "An Efficient Trust Management Algorithm in Wireless Sensor Network". © Springer Science+Business Media Singapore 2016. N.R. Shetty et al. (eds.), Emerging Research in Computing, Information, Communication and Applications, DOI 10.1007/978-981-10-0287-8_26.

[3] Mukesh Kumar and Kamlesh Dutta "A Survey of Security Concerns in Various Data Aggregation Techniques in Wireless Sensor Networks". Springer India 2015. L.C. Jain et al. (eds.), Intelligent Computing, Communication and Devices, Advances in Intelligent Systems and Computing 309, DOI 10.1007/978-81-322-2009-1_1.

[4] Vinod Kumar Verma, Surinder Singh, N. P. Pathak "Towards comparative evaluation of trust and reputation models over static, dynamic and oscillating wireless sensor networks". DOI 10.1007/s11276-015-1144-4. Springer Science+Business Media New York 2015.

[5] Weidong Fang, Chuanlei Zhang, Zhidong Shi, Qing Zhao, and Lianhai Shan "BTRES: Beta-based Trust and Reputation Evaluation System for wireless sensor networks". http://dx.doi.org/10.1016/j.jnca.2015.06.013. 1084-8045/& 2015 Published by Elsevier Ltd.

[6] X. Anita, M. A. Bhagyaveni, J. Martin Leo Manickam "Collaborative Lightweight Trust Management Scheme for Wireless Sensor Networks". DOI 10.1007/s11277-014-1998-2. © Springer Science+Business Media New York 2014.

[7] Yun Liu, Chen-xu Liu, Qing-An Zeng "Improved trust management based on the strength of ties for secure data aggregation in wireless sensor networks". DOI 10.1007/s11235-015-0078-6. © Springer Science+Business Media New York 2015.

[8] Yannis Stelios, Nikos Papayanoulas, Panagiotis Trakadas, Sotiris Maniatis, Helen C. Leligou, and Theodore Zahariadis "A Distributed Energy-Aware Trust Management System for Secure Routing in Wireless Sensor Networks". F. Granelli et al. (Eds.): MOBILIGHT 2009, LNICST 13, pp. 85–92, 2009. © ICST Institute for Computer Sciences, Social-Informatics and Telecommunication Engineering 2009.