An Efficient Web Services Framework for Secure Data Collection in Wireless Sensor Network

Venu Madhav Kuthadi[1], Rajalakshmi Selvaraj [2], Tshilidzi Marwala[3]
[1]Department of AIS, University of Johannesburg, South Africa
[2]Faculty of Engineering and the Built environment, University of Johannesburg, South Africa & Department of Computer Science, BIUST, Botswana
[3]Faculty of Engineering and the Built Environment, University of Johannesburg, South Africa
Email: venumadhav56@gmail.com

Abstract

In general, wireless sensor network consists of more number of low-cost sensor nodes which have particular sensing range, computation and communication capability. The amount of data transmission of sensor nodes should be reduced to improve sensor lifetime and overall bandwidth utilization. One of the techniques to improve the bandwidth lifetime and energy utilization is data aggregation in wireless sensor networks. Usually, wireless sensor network will implement in remote and hostile environment to transmit sensitive information. It is also used to protect from node compromise attacks and security issues such as data confidentiality and integrity. However, some techniques can be introduced to secure data transmission in wireless network. This paper introduces a new Hash and Time Based security approach for secure data transmission in the wireless sensor network**.** In the first phase, Web services are implemented in the sensor networks and the interaction between the systems is described using SOAP (Secure Object Access Protocol) messages typically conveyed into an XML (extensible Markup Language) serialization. In the second phase, secure transmission of data is achieved using hybrid algorithm. Finally the secured data is aggregated using Recoverable Concealed Data Aggregation Model.

Keywords: Wireless Sensor Network, Secure Data Aggregation, Hybrid Security Model, Web Service, Recoverable Concealed Data Aggregation

Introduction

(WSN) Wireless Sensor Network is commonly known as ad- hoc network. It consists of spatially scattered independent tiny sensor nodes which gather information from different environments by means of sensing or monitoring the events. Sensor nodes contain specific sensors, processor, wireless transceiver and battery. A restricted amount of power and a smaller amount memory is used only by the WSN because these networks operate on battery. The Wireless Sensor Network's important function is to observe, detect and forecast the real world events. Communication and Battery components are used by the wireless sensor nodes which sense the event change information from the real world environments and transmit the sensed information through wireless channel via additional nodes as well as to the corresponding designated base station or to the sink node. An access point from the base station gathers information which is transmitted to the human interface. Précising and merging sensor data is also termed a Data aggregation process that is used to minimize the

 ISSN 2047-3745

number of transmission in the WSNs. A low energy consumption network with secure data aggregation frame must be implemented to minimize the transmission cost in Wireless Sensor Network. This framework includes two novel techniques to protect the confidentiality of the sensed data and secure data aggregation at the sink node site.

A security method should be introduced in WSN to protect data transmission from attackers and unauthorized, unauthenticated WSN nodes. The important function is to manage the authenticity, integrity and confidentiality of the information that is transmitted among the nodes of the network. In numerous ways, the intruder can be attack the WSN nodes like interfering and overloading the information packets. Thus, it will impact on the data integrity, eavesdropping i.e., unauthorized accessing in the WSN and ensure the authenticated nodes must be accessing the data. For maintaining and administrating the Wireless Sensor Network, there are various routing protocols are used such as location-based, Hierarchical, flat-based, Mobility-based Network flow and QOS (Quality of Service), Heterogeneity-based protocols, Multi-path based.

As a result this research work addresses the security problem in the wireless sensor networks. This work also concerns the energy saving, power consumption and low cost. Recent works focus on the security mechanisms but they didn't achieve better results. A new technique is proposed for secure data aggregation and secure transfer of data. Rest of the work is discussed in the following sections. Section 3 explains the proposed architecture diagram with detail. Section 4 shows the results and discussion. Finally section 5 includes the conclusion and future work of our proposed work.

Related Work

Various studies have been made through wireless sensor network to protect secure data communication but the majority of them focusing on data aggregation technique with some secure protocols and algorithms for data transmission. A novel secure method is established to defeat the negative aspect of secure data aggregation technique. The outcome of various researches on privacy preserves data aggregation has been discussed below. A novel data aggregation framework is proposed by Jae-Woo Chang, Yong-Ki Kim, and Min Yoon. In order to guarantee the low power consumption and data security in WSNs. In WSN data security aggregation method is similar to the Hilbert curve in which a novel Tree-based wireless network arrangement is made to reduce the connectivity between the neighbor sink nodes for the sensor network construction. To protect the data privacy a novel technique called Hilbert curve is adopted which encrypt the transferred information via Hilbert value. Even if the attacker's eaves drop the transfer data it is complex to mark out the physical value. The exposure of the existing technique in terms of data security and power efficiency is outperformed in performance analysis.

A novel approach called protected routing in WSN is being framed and proposed by Jyoti Shukla, Babli Kumari. Detection based path hopping is a latest framework which protect wireless sensor network from attacks and intruders such as path hopping, with error, without error, are the different situations prevailing in the environment. The result shows that the ratio of the path delivery from the original path hopping technique is less than the ratio of packet delivery ratio of detection based path hopping technique. Thus, it provides more security than the existing path hopping technique.

A novel framework in WSN for secure data recovery and aggregation is being proposed by Akuluri Rakesh, J. Shajin Prince and John Major. To overcome the negative aspect of integrity and authenticity in the sensed data.. The primary function which the data recovery try to provide is the sink node which check the authenticity and integrity of sensed information and secondly the sink node which can execute the process of aggregation in the data. The proposed system is protected under our attack model. The outcome of the proposed work proves to the fact that it is inexpensive and reasonable.

An innovative design called A Secure Hop by Hop Data Aggregation Protocol which is being proposed by Guohong Cao, Sencun Zhu, Yi Yang and Xinran Wang for WSN and the design SDAP is founded mainly from the values of attest, commit, divide-and-conquer. Initially, SDAP uses a heuristic probabilistic grouping technique to dynamically partition the nodes in a tree topology into many logical sub trees of same sizes. Hop by hop aggregation is performed in every group to produce a group aggregate in a conditional manner. The sink node recognizes the doubt full group from the set of aggregate groups. At last all the set aggregate take part in the verification process to show the accuracy of their aggregate groups. The simulation and research work prove that the SDAP has attained the stage of effectiveness equal to regular hop-by-hop aggregation protocol. It offer some guarantee on the aggregation Integrity outcome.

Protected Reference Based Data Aggregation Protocol is a novel technique in WSN proposed by Guttikonda Prashanti and Miriyala Markandeyulu in which they give a secure susceptibility of data aggregation for systems, and a study on strong and protected aggregation protocols that are flexible to provide fake data insertion attack. From this proposed work we can get complete information about the protected data aggregation in WSN i.e. In wireless sensor network, the affiliation among security requirements and data aggregation conception are clarified and a wide survey of literature is given by cutting the state-of-the-art data aggregation protocols.

A novel survey in wireless sensor network called Energy Efficient Routing via Balanced Clustering proposed by, Dionisis Kandris et al (ECHERP) Equalized Cluster Head Election Routing Protocol is the most recent protocol which follows power preservation via balanced clustering. To improve the network lifetime ECHERP represents the network as a linear system and using Gaussian elimination algorithm it calculates the combination of nodes chosen as cluster heads to improvise the network lifetime. In ECHERP the performance assessment is done with the help of replication test where the efficiency of the protocol in terms of network energy efficiency when compared against other well-known protocols.

In WSN, Sudharshan Tiwari, Sanjeev Jain, Vinay kumar proposed a new frame work on Energy Efficient Clustering Algorithms. The timeline and explanation of LEACH Protocol and its descendant are given in wireless sensor network. In WSN, the study of LEACH and descendant along with the various clustering algorithm networks is reported in the literature.

It has been established that the networks natural life maximized by the power efficient algorithms even though many efforts are performed to give a finished and correct state of the art survey on energy efficient clustering algorithms along with LEACH and its descendant as applicable to WSNs.

In Wireless sensor network, Computational Intelligence Based Data Aggregation method in Clustered is framed and proposed by Muhammad Umar Farooq. In this technique, for producing effective data aggregation it is necessary to find a non-conventional explanation like CI. From this technique we can find the consumption of computational intellect and its

prototype in data aggregation and fusion which is discussed. It desires a centralized approach where the data's are collected from the central node for performing processing and communicating results. This collected information gives an outcome of the maximized transmission cost. Data fusion opposing to it is frequently perform once the data has been grouped at the cluster head or the BS, which makes the approach fit matched.

In WSN, a data Aggregation technique is being framed by S. Patil, P. R. Patil, Nandini with the Aim of comparing the performance of the TAG in wireless sensor network by balancing in terms of power efficiency along with or without data aggregation and to assess the correct protocol in an environment where resources are very few. The major important areas of data transmission in wireless sensor networks like query processing, data aggregation and understood how communication in wireless sensor is unique from other wireless sensor. The replicated outcome illustrate that the information from source node is transferred to sink node via neighbors nodes in a multi hop fashion by minimizing the communication and getting energy, the power usage is less when balanced with that of the transferred data in straight to the base station i.e. aggregation reduce the data communication without aggregation. From the above mentioned process aggregation is effectively performed in WSN. Various problems like reference based, clustering, hop by hop, bit error rate, path hoping technique, data recovery model etc., are being reported in the research work .To overcome the issue of giving protected data communication and aggregation certain novel secure algorithms can be introduced. A latest arithmetical method is framed in this survey, in which privacy preserve data transmission and aggregation via hybrid algorithm approach. This outcome is balanced with existing method.

Proposed Work

The Architecture diagram consists of a set of spatially divided sensor nodes, sink node, and user of the sink node. Each and every node is connected with wireless sensor network. The sensor nodes contain sensor devices such as battery and memory devices in addition to that some devices which are used for web service are also fixed with it. The sensor device will absorb the events or measures and store in the memory devices. A transceiver fixed with the device will transmit the absorbed events or measures to other nodes and to the sink node. Web services are implemented with every sensor nodes for efficient data transfer.

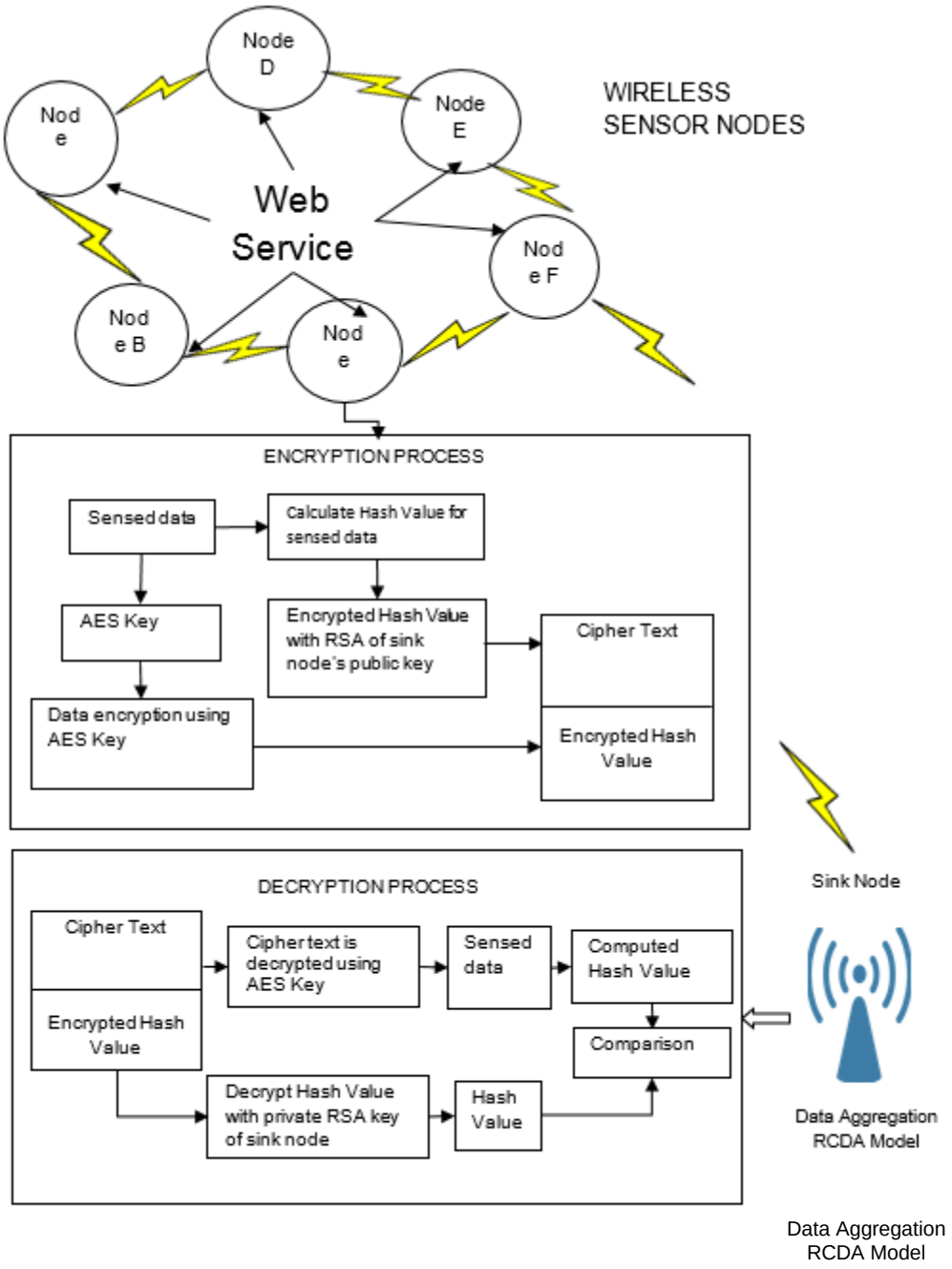

Fig. 1 Proposed Architecture

The above architecture consists of six nodes namely A, B, C, D, E, and F. These nodes will transfer the data to the sink node by the neighboring nodes. The node A wants to send the data to the sink node and it will transfer the data to the neighbor node D. Similarly the D node will transfer the data to the next neighbor node F. The node F only collects all the data from the nodes and transfers it to the sink node. The collected data's are transferred through SOAP Messages to the sink node.

In the encryption process the collected data is converted into XML form and encrypted using private AES (Advanced Encryption Standard) key. A Time Stamp and a hash value are fixed with the SOAP Message. The hash value is generated by the SHA 256 (Secure Hash Algorithm) algorithm and the hash value is encrypted using public RSA (Rivest Shamir Adleman) key. The SOAP message will transfer the data to the neighbor nodes and to the sink node. The message is fixed with Hash Value and a Time stamp. The hash value and Time stamp of received node is compared with the hash value and the time stamp is already fixed with that node. If the Hash value and Time stamp values matches with the value which is already fixed with the node then the message will be automatically forwarded to next neighboring node. If the value in the received message does not match with the node values then the message will be discarded.
Decryption process is the reverse of encryption process the encrypted data is decrypted using private AES key and the original content is obtained at the sink node. At the sink node the original data's are aggregated using RCDA model. RCDA will recover the sensor data generated by the sensors even if the data is aggregated by cluster heads. The data is recovered by finding the integrity and authenticity of sensing data and the base station will execute some aggregate functions on the data.

Web service in wireless sensor networks

The sensor networks are focusing on heterogeneous devices supporting a large range of applications. A new architecture approach is proposed for providing secure data transmission between the sensor node and the sink node. Web Service is designed to support interoperable machine to machine interaction over a network. Wireless Sensor Network interaction with web service is described using SOAP messages with an XML serialization.

Securing Sensor Data

The sensor nodes will sense or observe the events or measures and store in the memory device. The stored data is transmitted to the sink node by neighboring nodes. Data transmission in wireless device does not provide security. For ensuring security some security algorithms should be used during transmission. A new Hybrid Algorithm is proposed to secure the data during transmission.

Hybrid Approach

The Hybrid algorithm is the combination of AES and RSA algorithm. The data is encrypted using AES algorithm and a hash value is generated by using SHA 256 algorithm. The hash value is encrypted using public RSA algorithm. The data is decrypted by the reverse process of encryption.

Data Encryption

In the encryption process the data's to be transmitted is encrypted using AES algorithm. AES encryption includes four process they are substitution bytes, shift rows, mix columns and add round keys. The input data or the plain text is divided into 128 –bit blocks. Each block will

have binary value less than a number n. The block size should be less than or equal to log2 (n). Suppose if block size is 2^k bits where 2^k<n=2^k+1. The encryption of plain text block is M and cipher text block is C then,

$c = M^e \bmod n$

A Hash value is generated using SHA-256 algorithm and the hash value is encrypted using RSA algorithm. The RSA encryption includes two steps they are key generation and encryption. The key generation procedure includes,

1. Generate two large distinct prime numbers x and y
2. Calculate n = xy such that ϕ= (x − 1) (y − 1).
3. Select e, such that 1 < e <ϕ, relatively prime toϕ.
4. Calculate integer i, such that 1 < i< ϕ where ei≡(1.
5. Return public key (n, i) and private key d.

The encryption procedure of RSA algorithm is

1. Let us represent an integer message M such that {0<M<1}
2. Calculate the cipher text QUOTE

Where C is cipher text and M is encrypted message.

The hash value and a time stamp are fixed in the SOAP message. The encrypted data is converted into XML document by SOAP messages. The SOAP message transfers the data to neighbor node.

Data Decryption

The new neighbor node will contains the already stored private RSA key and Time stamp. This node will match the stored private RSA key and the Time stamp with the received message. If the key and the time stamp are matched with the received message header then this message will be automatically forwarded to the next neighbor node otherwise the message will be discarded. This process will be continued until every routing node received the message and finally the sink node will receive the SOAP message. The Decryption process is the conversion of cipher text into plain text. The sink node decrypts the hash value by its private RSA key by using the equation

$M = C^d \bmod n.$

The plain text is decrypted using the AES decryption key by,

$M = C^{ed} \bmod n$

Where M is plain text and C is cipher text.

Steps followed in proposed Hybrid Algorithm

Step1: Sensor S sensing the value V.
Step2: Compute the Hash value of sensing value.
Step3: Encrypt the Hash Value using RSA Encryption Method with public key
Step4: Encrypt the sense data value using AES encryption method with symmetric key
Step5: Send the above information using SOAP protocol with time tag element
Step6: Sink node check the received message with time stamp.
Step7: If matched proceed to next step otherwise ignore.
Step8: Decrypt the hash value using its private RSA key.
Step9: Decrypt the plain text using AES algorithm.
Step10: Continue step 6 to 9 for every received message.

Data Aggregation: Statistical Model

Different types of Sensors used to sense different measures such as temperature, light, humidity, pressure etc. The data collected at the sink node will have some errors due to some effects includes noise, distortion and environmental effects. The collected data's from the sensor nodes are valuable and sensible. It will be used by the user for various experiments and researches. A statistical model is introduced to calculate the error rate of the received data. In this model the total error rate is calculated by processing the input sample data with corrected error data to the total amount of corrected error data. A distributed total range of sample values are generated for every testing of received data. The sample values are applied to error input data to corrected error data to the total amount of corrected error data. By applying these sample values to error occurred data's the total error rate will be measured.

If Xs is the sample error data obtained by the sink node and Xc is the corrected error data obtained by the observed error data to the predicted error data. The Total Error Rate is calculated by,

$$Eout = 100.\sqrt{\frac{1}{NN}.\sum_{i=1}^{NN}\frac{|Xs(i)-Xc(i)|^2}{|Xc(i)|^2}}$$

Where NN is the total number of sample values. Xs(i) is the sample error input data generated by the sensor, Xc(i) is the corrected error data.

Recovering Loss Data

A new data aggregation technique called Recoverable Concealed Data Aggregation (RCDA) is introduced. In this method the data generated by the sensor nodes can be recovered in the base station or the sink node. RCDA will recover the sensor data generated by the sensors even if the data is aggregated by cluster heads. The data is recovered by finding the integrity and authenticity of sensing data and the base station will execute some aggregate functions on the data.

The sensor nodes collect the data and transmit the data to the sink node using the proposed hybrid algorithm for secure data transfer using web services. The sink node collects the data and aggregates it with RCDA mechanism. Finally the aggregated data is processed to produce the results.

Results and Discussion

Hybrid security algorithm provides secure transmission of data between the sensor node and the sink node. The structural model will calculate the error rate of this proposed work. The obtained results are calculated with Total number of sensors, power consumption, Encryption Time, Compromised data and Error Prediction rate and their performances are measured.

Experimental Setup

The experimental setup consists of six nodes that absorb data and a sink node to collect the received data fixed in an environment. Every node is separately fixed at a distance of 15

meters and 5 unit of energy is assumed to all the nodes. For every minute the sensor nodes transmit 10 kb of data to the sink node. Web Services is implemented in all the sensor nodes for data transfer and these sensor nodes will transfer the encrypted data to sink node via SOAP message. The sensor data is securely encrypted by using Hybrid algorithm for secure transmission. The transmitted data's at the sink node are decrypted and finally aggregated using RCDA method. At last, the simulations of this experiment shows efficient data transmission and obtain more security in the network

Number of Sensors Vs Power Consumption

The figure 2 shows the energy consumption of various quantity sensors. The proposed wireless sensor network model consumes less energy because of using Web Services.

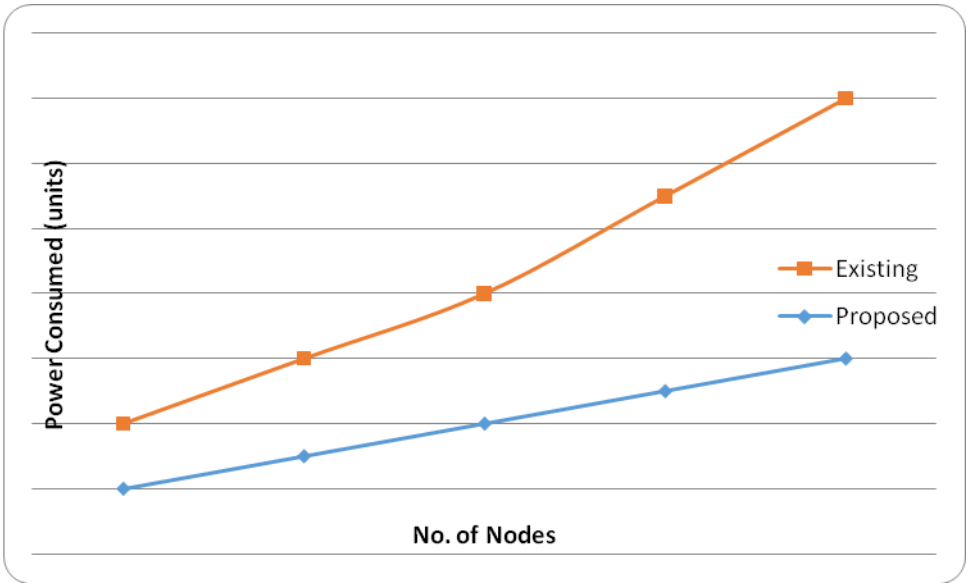

Fig. 2. Number of Sensors Vs Power Consumption

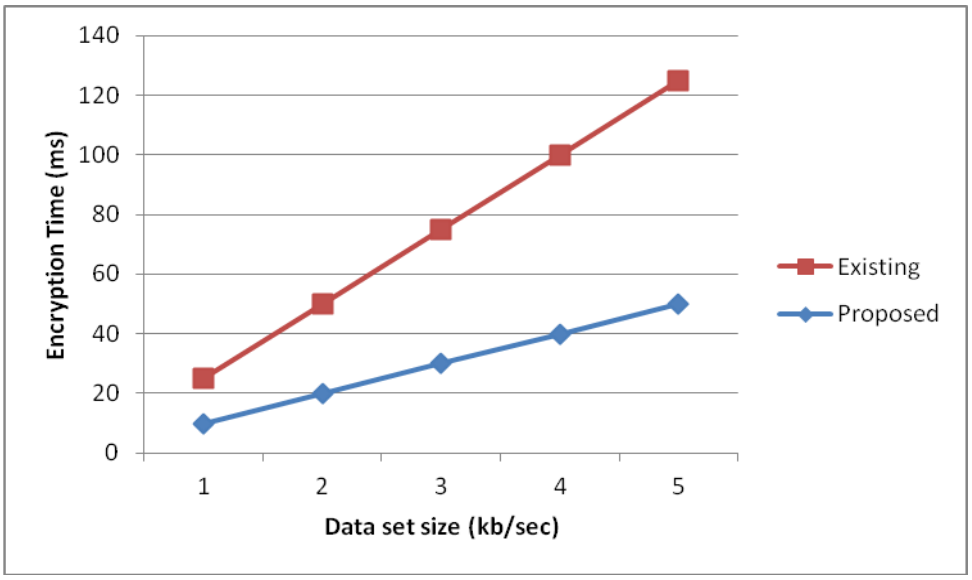

Fig. 3: Data set Size Vs Encryption Time

The figure 3 shows the effective encryption done in the system. It shows that the time for encryption is very low when compared to existing systems**.**

Total Sensors Vs Compromised Data

The figure 4 shows that the compromised data in the total sensor. The data compromised level is less in the total deployed sensors.

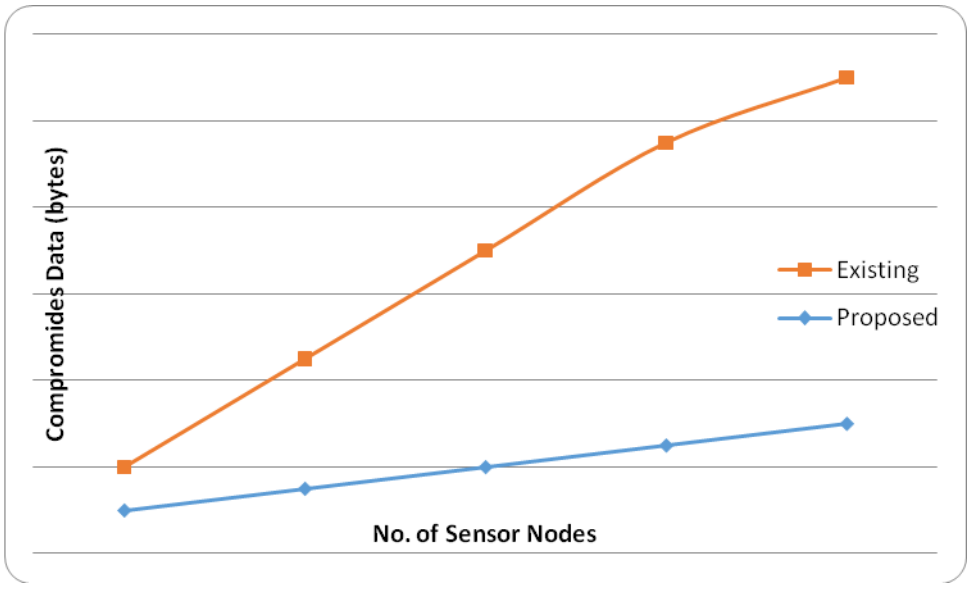

Fig. 4: Total Sensors Vs Compromised Data

Data Vs Error Prediction Rate

The figure 5 represents the total error predicted in the wireless sensor network system. The error rate is computed with original data that is received from various sensors. The comparison shows that the error rate prediction is very high compared to the existing system.

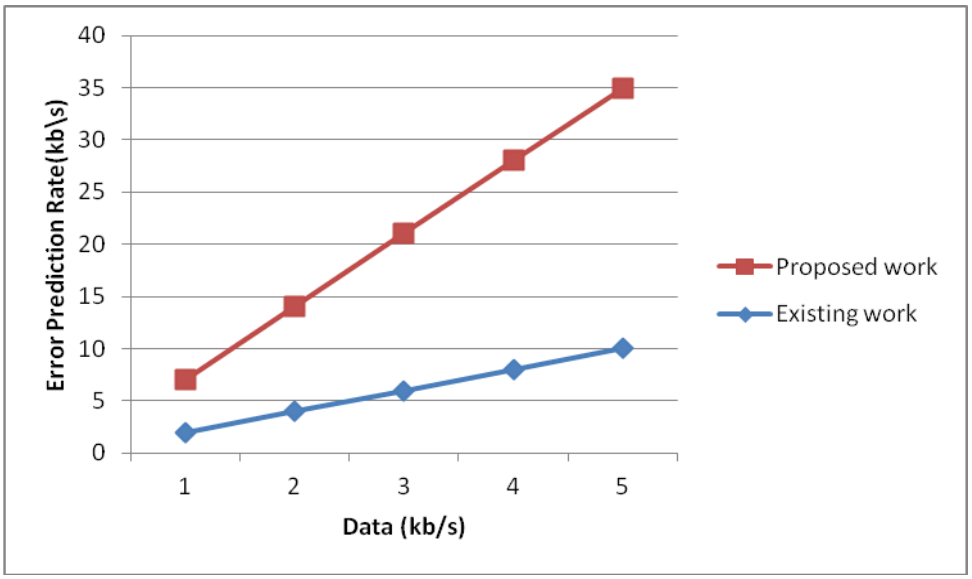

Fig. 5: Data Vs Error Prediction Rate

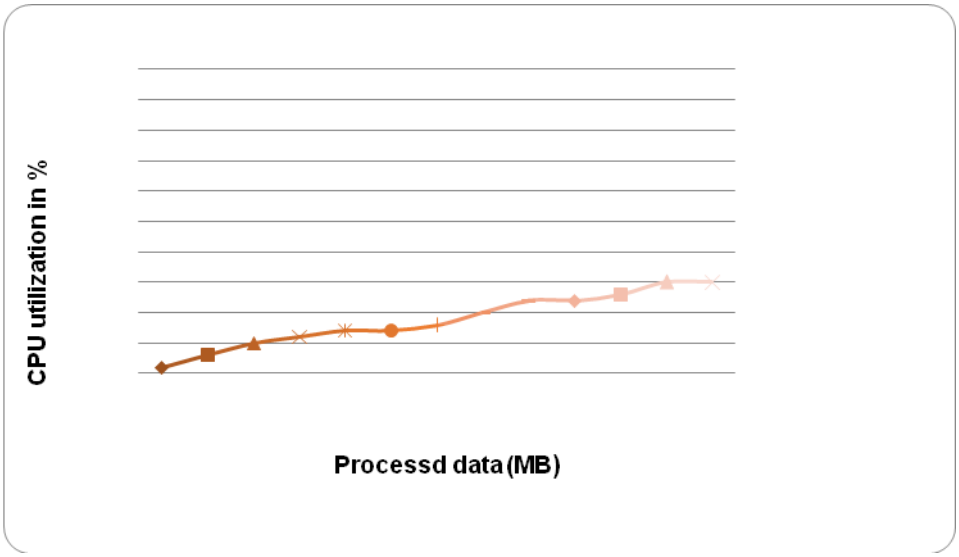

Figure 6 comparison of processed data with CPU utilization.

This indicates that the proposed method produces efficient CPU utilization and the processing speed is also increased.

Table 1: Detected Error from Received Data with computational Time

Data Set Size(mb)	Error Rate(mb)	Computation Time (ms)
20	**1**	**15**
40	**2**	**30**
65	**3**	**35**
80	**3**	**45**
100	**4**	**50**

Table1. Represents the total error data occurred in dataset and computation time of data. The error occurrence rate is lower for the received data and the computation time is also very low.

Conclusion and Future Work

This paper provides an efficient secure data aggregation between wireless sensor nodes and the sink node. The modified hybrid algorithm provides high secure data transmission between wireless sensor nodes. The proposed method effectively transmits the data to the sink node using web service model and also this model provide efficient data structure to verify sensed data. Also, the proposed work reduced more power consumption, total error rate and also increased processing speed effectively. The future work involves extending the web service for reliable transmission between sensor nodes.

References

Miriyala M,Guttikonda P. Secure Reference Based Data Aggregation Protocol for Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering.2013:2(7):978-983.

Fasolo E, Rossi M, Widmer J, Zorzi M. In-network aggregation techniques for wireless sensor networks: a survey, IEEE Wireless Communication Journal. 2007:14(2):70–87.

Rajagopalan R, Varshney PK. Data-aggregation techniques in sensor networks: a survey. IEEE Communication Surveys. 2006:8(4):48-63.

Selvaraj, R., Kuthadi, V.M. & Marwala, T. (2015). An Effective ODAIDS-HPs approach for Preventing, Detecting and Responding to DDoS Attacks. *British Journal of Applied Science & Technology*, Vol.5 (5): 500-509.

Stefanos AN, Dionisis K, Dimitrios DV, Christos D. Energy Efficient Routing in Wireless Sensor Networks Through Balanced Clustering.Article Algorithms.2013:6(1):29-42.

Yueshun H, Zhang W. The research on Wireless Sensor Network for Landslide Monitoring.International journal on smart sensing and Intelligent Systems. 2013:6(3):867-887.

Babli K, Jyoti S. Secure Routing in Wireless Sensor Networks. International Journal of Advanced Research in Computer Science and Software Engineering. 2013:3(8):746-751.

Min Y, Yong-Ki K, Jae-Woo C. A New Data Aggregation Scheme to Support Energy Efficiency and Privacy Preservation for Wireless Sensor Networks.International Journal of Security and Its Applications. 2013:7(1):129-142.

John M, Shajin P, Akuluri R.Secure Data Aggregation and Data Recovery in Wireless Sensor Networks. International Journal of Engineering and Advanced Technology. 2013:2(3):271-275.

Yi Yang, Xinran W, Sencun Z,Guohong C.SDAP: A Secure Hop-by-Hop Data Aggregation Protocol for Sensor Networks. ACM Transactions on Information Systems Security. 2008:11(4):18-43.

Vinay K, Sanjeev J, Sudarshan T. Energy Efficient Clustering Algorithms in Wireless Sensor Networks: A Survey. International Journal of Computer Science Issue 2011:8(5):259-268.

Muhammad UF. Computational Intelligence Based Data Aggregation Technique in Clustered WSN: Prospects and Considerations. Proceedings of the World Congress on Engineering and Computer Science. San Francisco.2012.

Nandini SP, Patil .PR. Data Aggregation in Wireless Sensor Network. IEEE International Conference on Computational Intelligence and Computing Research, India 2010.

Takayama S, Akiyama J, Fujiki T, Mokhtar. Wireless Sensing Network Management for Landslide Disaster Monitoring Measurement, Proceedings of the 9th International Conference, Smolenice, Slovakia. 2013:259-262.

Kemal A, Mohamed Y. A survey on routing protocols for wireless sensor networks. Ad- Hoc Networks, 2005:3(3):325-349.

Kuthadi VM, Rajendra C, Selvaraj R. A Study of Security Challenges in wireless sensor networks, Journal of Theoretical and applied technology. 2010:20(1):39-44.

Dr. Prerna Mahajan & Abhishek Sachdeva, "A Study of Encryption Algorithms AES, DES and RSA for Security", Global Journal of Computer Science and Technology Network, Web & Security Volume 13 Issue 15 Version 1.0 Year 2013.

John Major. J, Shajin Prince, Akuluri Rakesh, "Secure Data Aggregation and Data Recovery in Wireless Sensor Networks", International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-3, February 2013.

Nils Gruschka, Meiko Jensen, Luigi Lo Iacono, and Norbert Luttenberger, "Server-Side Streaming Processing of WS-Security", "IEEE Transactions on services computing" , Vol. 4, No. 4, October--December 2011.

Authors Profile

1. DR VENU MADHAV KUTHADI currently working with University of Johannesburg, he obtained his PhD degree in computer science from MU India. He received his Master's Degree in Computer science from JNTU India. He got 14 years of Experience in research and teaching undergraduate and postgraduate students of Engineering. He holds B.Tech in CSE from ANU India. He has published good number of articles in international journals and conference proceedings. Dr Kuthadi is an Editor for the International journal IJAEGT.

2. DR RAJALAKSHMI SELVARAJ is currently working as academic staff in the department of Computing, BIUST, Botswana. She has received Ph.D from Magadh University, India. She has M.Phil in Computer Science from Periyar University, India. She did Master's (MCA) degree in Computer Science from Madras University, India and Bachelors (B.Sc) Degree in Computer Science from Madras University, India. She has 10 years' experience of teaching undergraduate and postgraduate students of Computer Science

3. PROFESSOR TSHILIDZI MARWALA is a deputy Vice Chancellor at the University of Johannesburg. He was previously the Executive Dean of the Faculty of Engineering and the Built Environment at the University of Johannesburg, the Head of Control and Systems Group and the Carl and Emily Fuchs Professor of Electrical Engineering at the University of the Witwatersrand, Executive Assistant to the Technical Director at the South African Breweries, Chair of the (Telkom) Local Loop Unbundling Committee, Deputy Chair of Limpopo Business Support Agency, director of the State Information Technology Agency Pty (Ltd), member of council of Statistics South Africa and member of council of the National Advisory Council on Innovation. He has been on the boards of City Power Johannesburg Pty (Ltd) and EOH Pty (Ltd). He holds a Bachelor of Science in Mechanical Engineering with a Magna Cum Laude from Case Western Reserve University, a Master of Engineering from the University of Pretoria, a PhD in Computational Intelligence from University of Cambridge and was a post-doctoral research associate at the University of London's Imperial College of Science, Technology and Medicine. He has received over 40 awards including the Order of Mapungubwe; has published over 150 articles in refereed international journals, conference proceedings and book chapters and has successfully supervised over 33 master and PhD students