DOI: http://dx.doi.org/10.26483/ijarcs.v9i2.5645

Volume 9, No. 2, March-April 2018

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

HOMOMORPHIC ENCRYPTION ALGORITHM USED FOR SECURITY ENHANCEMENT IN WIRELESS SENSOR NETWORK CONTENT-BASED ROUTING

S. Veerappan
M.Sc Project Student
Department of Information Technology
Bharathiar University
Coimbatore-46, India

Dr. R. Vadivel
Assistant Professor
Department of Information Technology
Bharathiar University
Coimbatore- 46, India

Abstract: Wireless sensor network deals with communication based on wireless. It enables distributed frameworks to be outlined and executed in a self-sufficient route by advancing the development procedure. Utilizing self-sufficient objects gives new method to effective processor and memory use while empowering low-control utilization in communication. In this paper we propose a protocol which was based on content-based to take care of some characteristic issues in wireless sensor networks, particularly in correspondence. The protocols based on content are primarily amplified the rate of appropriate message conveyance and limit the energy utilization by utilizing strategies to keep up briefest ways. It passes information by utilizing a platform based on agent, where every sensor can take on its choice separately. This protocol extends the network lifetime. When the nodes gets dead, the system consequently build new route for sending data. Also, this proposed work utilizes Homomorphic encryption for security purpose. Performance evaluations are done using efficiency metrics and it can be utilized for evaluating the lifetime of the system.

Keywords: wireless sensor networks, Agent-based platform, content based routing protocol, Homomorphic encryption.

1. INTRODUCTION

Currently the usage of Wireless Sensor Networks (WSNs) gets increased in various application regions, by cooperatively the sensor nodes can sense the environment and transmit the detected information to its base station. It is as yet a testing issue to accumulate, convey and process these information enough in a energy proficient way. Occurrence driven distribute frameworks are viewed as proficient way for gathering of data and sending errands in WSN. Data can be passed on simply when specific occasions happen. Contrasting with request/response design, information exchange occurs by sending requests and waiting for response.

WSNs are intelligent compared with traditional sensors, and some WSNs are sensed data can be gathered in situ and transformed to more abstract and aggregated high-level data before transmission. The blend of the power of processing, storage, and wireless communication implies that information can be acclimatized and spread utilizing keen algorithms [1], [5]. Also, many applications utilize wireless sensor nodes and suggest a noteworthy part of these systems would need to get the self-association ability. TCP protocols developed for the traditional wireless networks are not suitable for WSNs where the notion of end-to-end reliability has to be reinterpreted due to the “sensor” nature of the network which comes with features such as: Multiple senders, the sensors, and one destination, the sink. For the same event there is high level of the redundancy or correlation in the data collected by the sensors. On the other hand there is need of end-to-end reliability between the sink and individual nodes for situations such as re-tasking or reprogramming. The protocols developed should be energy aware and simple enough to be implemented in the low-end type of hardware and software of many WSN applications [2]. The constructed encryption methods that can evaluate and perform own decryption and the call scheme that can evaluate decryption circuit boost trappable. Then lattice-based are crypto designed to use in-network processing.

2. RELATED WORK

The predictive storage architecture for emerging large-scale, hierarchical sensor networks is shown in WLAN monitoring system [3]. Rather than existing procedures, proxy-centric architecture where fastened by gathering the requirement for intelligent questioning from clients with energy enhancement needs of the remote sensors. The principle oddity in this work lies in the broad utilization of prescient methods that are a characteristic fit to the corresponded conduct of the physical world. The endeavors innovation inclines away to assemble engineering stress chronicled at remote sensors and astute reserving at intermediaries. They can be utilized as a part of various routes in various application settings. Natural climate examples and suburbanite activity designs are cases of information that are exceptionally unsurprising in the basic case. Prescient can empower the framework to monitor vitality by taking in the anticipated parts of the information, and proficiently removing just the unusual data from remote sensors [4]. Reconnaissance applications can utilize the documented ability of prescient to an inquiry for occasion logs relating to past occasions.

A Fully Homomorphic encryption scheme that allows pattern in which knowledge exchange happens by issuing requests and waiting for suitable answers, system typically decryption algorithms often demanded with low circuit complexity in product lattices provided both the multiplicative homomorphism's (a public key ideal in a polynomial ring that is represented as a lattice.) The scheme is not quite boots trappable scheme can correctly evaluate can be logarithmic in the lattice dimension. The decryption circuit, but the latter is greater than the formulation. In the final step, the modify the scheme to reduce the depth of the decryption circuit.

3. USED ALGORITHM

Proposed system provides the semantic security for Hybrid routing protocols in wireless sensor network. Once the system is semantically secured it is not possible to retrieve the content of the query message by simply hacking the key. Such semantic security is implemented using the Fully Homomorphic encryption algorithm is used. This system effectively handles all type of security threads. It also provides resiliency,

Where

M is the packet with payload and packet headers

Source M $\xrightarrow{\text{Homomorphic encryption}}$ **Destination M|**

Compute for payload and
Packet header

M| is updated periodically using f(x) w.r.t to Time is denoted as p^{o}

Publish /subscribe model can decrease the network overload significantly. The provided a general result support to the construct a used to encryption scheme that primitives Evaluation of Arbitrary circuits, it suffices to flexible-time authentication and source identity protection without the threshold limitation. Provide semantically secured by wireless sensor network.

A. Algorithm – fully Homomorphic Encryption

Apply confidential preserving to user data through fully Homomorphism encryption which Is attribute based model
Single user data = Attribute
Example
IP address = Attribute
File type = Attribute
Location of the Packet (packet header) is also secured by encrypting the source and designation identity of the routing table periodically against DDOS
Attribute based Encryption
Generate the Cipher Text to the Attribute through Anonymization
Anonymization is right Shift or Left shift with string index to the data
Data = "192.168.1.106"
Applying Indenting technique which a Encryption logic
Shift = right
Shift level -2
Index -13
Cipher Text = "192.168.1. 108"
X denotes the time
$P^{o} = f(x)$
Cipher text for Homomorphic encryption is given by €
∂ --→Original payload or packet header
$€ = ∂ + £$
Where £ is encryption logic based attributes of data
$£ = \sum \alpha$

4. METHODOLOGY

The WSNs are counterfeit to subsist of a large number of sensor nodes. We accept that every sensor nodes have knowledge on its relative area in the sensor space and is fit for interfacing with its neighboring nodes specifically utilizing geographic directing

a. Development of Wireless Network

The whole system is completely connected through multi-hop interchanges. We expect there is a security server (SS) that is in charge of development, storage and dispersal of the security parameters among the system [7].WSNs are intelligent compared with traditional sensors, and some WSNs are has capability of functioning in terms of creating a data, receiving the data and transmitting information over the communication channel. In the network, distribution frame and patch panel cannot be treated as computing node. The Similarity between the traces is carried out using pair wise similarity Matrix. Traces are connected in graph passion. The fully routing table is updated with Anonymization through Homomorphic encryption against the eaves dropping, brute force attack designed to use in network processing, where sensed data can be gathered in situ and transformed to more abstract and aggregated high-level data before transmission. The tremendous number of sensor nodes made arrangements for some applications and additionally suggests a noteworthy segment of these systems would need to secure self-association capacity.

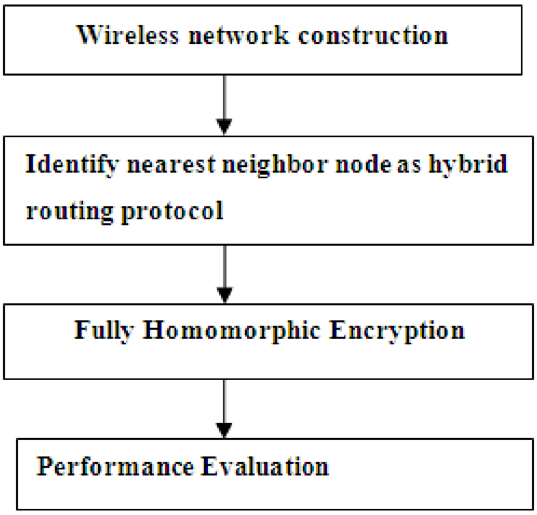
Wireless network construction
Identify nearest neighbor node as hybrid routing protocol
Fully Homomorphic Encryption
Performance Evaluation

Fig 1: Modular Structure

a. Identify nearest neighbor node as hybrid routing protocol

In graph passion, the fully connected graph is used to represent the traces , traces similarity is calculated from it , in graph model vertices represents the trace and weight represent no of similar occurrence of the traces using matrix calculation. Monitor repositioning can be particularly useful in spontaneous wireless networks such as ad hoc networks in general, as they do not count on any central entities that could be used as monitors [6]. Selecting a subset of traces can improve scalability, the extracting the subset of the most representative traces helps to reduce the number of merging operations (which are costly) [11]. Although the subset selection procedure adds complexity to the system, it is executed less often than the whole merging procedure.

b. Fully Homomorphic Encryption

The Fully Homomorphic encryption would leverage sensitive signatures in a host-based system. Address can use to challenges of monitoring encrypted sensitive networks. Signature is based on recent advanced in practical fully Homomorphic encryption practical in the guard. The success of this technology would enable broader use of cloud computing technologies and it would make existing host-based monitoring capabilities more effective by permitting the secure use of sensitive signatures [12]. The enable the cloud reduce the sensitive data leave on the information domain

c. Performance Evaluation

Node can be treated as data communication equipment or Data terminal equipment or as connection point, Source node, intermediate source for data transmission and terminal.

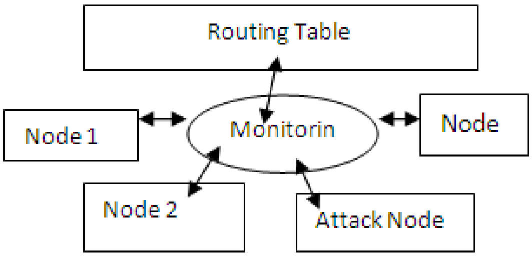

Fig 2: Flow Diagram Performance Evaluation

An Advanced routing procedure is utilized for choosing best route in a system. Directing was additionally used to mean sending system activity among systems [9]. In PSN (packet switching networks), routing coordinates packet sending through intermediate nodes. The routing procedure ordinarily coordinates sending based on directing tables which keep up a record of the courses to different system sources and goals [8]. It is essential for a proficient routing convention. Most steering calculations utilize just a single system way at the time. Multipath routing systems empower the utilization of numerous elective ways [10]. The information security systems for completely Homomorphic encryption are connected remote sensor organize. It will enhance the precision and less tedious. The outcomes are talked about in Experimental Result part.

5. SIMULATION ENVIRONMENT

This project developed using Java language and Java Netbeans simulator is used. Java networking programs are used for data transaction and Packet delivery. The distribution of the JDK includes the java SE bundle of NetBeans IDE (Integrated Development Environment), which is a powerful integrated development environment for developing applications on the Java platform. Using the Java EE platform Enterprise Edition (Java EE), users can develop applications more quickly and conveniently than in previous versions. Java EE significantly enhances ease of use providing

- Reduced development time
- Reduced application complexity
- Improved application performance

  Java EE provides a simplified programming model, including the following tools:
- Inline configuration with annotations, making deployment descriptors now optional
- Dependency injection, hiding resource creation, and lookup from application code
  - Java persistence API (JPA) allows data management without explicit SQL or JDBC
  - Use of plain old Java objects (POJOs) for Enterprise Java beans and web services

Table 1: Simulation Parameters

Software Requirements			***Hardware Requirements***	
IDE	Net beans		Processor	800MHz Intel Pentium III or equivalent
Developer tool	Java SE Development Kit (JDK)		Memory	350 GB
Operating system	Windows		RAM	1 GB
Java Library	Java FX Support			
Database	Java DB			
Language	Java EE			

6. PERFORMANCE EVALUATION

The experimental result we use to compare Homomorphic and symmetric key encryption algorithm. The proposed approach we got good accuracy and security strength in Homomorphic encryption. Homomorphic algorithms produce less time consuming.

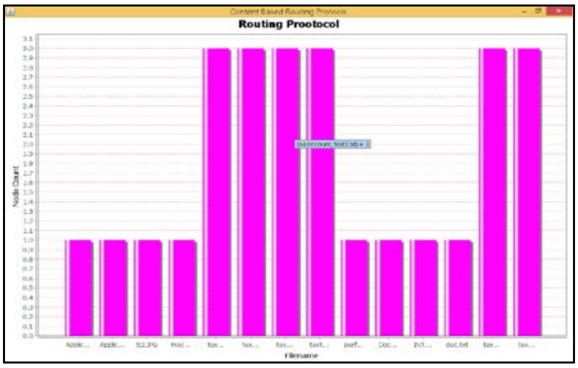

Fig 3. Graph of Network Node count

Table 2: Number of files Tested

Filename	***Node count***
52.JPG	1
Application Project List new.doc	1

ApplicationProjects.docx	1
Document.txt	2
Frecca.txt	3
INTRODUCTION.docx	1
performence_metrics.txt	1

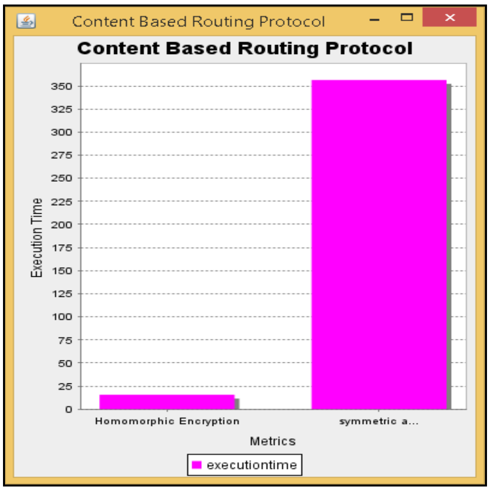

Fig 4. Graph of Execution Time

Table 3: Execution Time variation

Algorithm name	***Execution Time(ms)***
Homomorphic Encryption	15.625
Symmetric Key	356.375

7. CONCLUSION

The obtained features are provided for the classification process helps in classifying the data depend on the predicted results. The symmetric key technique performs better than the Homomorphic encryption. The symmetric key are get implemented for better analysis for various data set in a quicker manner. The accuracy of the classification is obtained in the better way to support various data sets with effective prediction provided by the classification process.

REFERENCES

[1] P. A. K. Acharya, A. Sharma, E. M. Belding, K. C. Almeroth, S. Member, and D. Papagiannaki, “Rate adaptation in congested wireless networks through real-time measurements,” IEEE Transactions on Mobile Computing, vol. 9, no. 11, pp. 1535–1550, Nov. 2010.

[2] Y. Sheng, G. Chen, H. Yin, K. Tan, U. Deshpande, B. Vance, D. Kotz, A. Campbell, C. McDonald, T. Henderson, and J. Wright, “MAP: a scalable monitoring system for dependable 802.11 wireless networks,” Wireless Communications, IEEE, vol. 15, no. 5, pp.10–18, October.

[3]. K. Tan, C. McDonald, B. Vance, C. Arackaparambil, S. Bratus, and D. Kotz, “From MAP to DIST: the evolution of a largescale WLAN monitoring system,” IEEE Transactions on Mobile Computing, vol. 99, no. PrePrints, p. 1, 2012.

[4] MatteoSammarco, Miguel Elias M. Campista, and Marcelo Dias de Amorim “Scalable Wireless Traffic Capture Through Community Detection and Trace Similarity” in IEEE TRANSACTIONS ON MOBILE COMPUTING vol.15, issue July 2016

[5] U. N. Raghavan, R. Albert, and S. Kumara, “Near linear time algorithm to detect community structures in large-scale networks,” Physical Review E, vol. 76, no. 3, pp. 036 106+, Sep. 2007.

[6] A. Argyriou and V. Madisetti, “Using a New Protocol to Enhance Path Reliability and Realize Load Balancing in Mobile Ad Hoc Networks,” Ad Hoc Networks, vol. 4, pp. 60-74, 2006.

[7] A, Bletsas, A. Khisti, D.P. Reed, and A,Lippman, “A Simple Cooperative Diversity Method Based on Network Path Selection,” IEEE J. Selected Areas in Comm., vol. 24, no. 3, pp. 659-672, Mar. 2006.

[8] V. Venkataramanan, X. Lin, L. Ying, and S. Shakkottai, “On Scheduling for Minimizing End-to-End Buffer Usage over Multi- Hop Wireless Networks,” Proc. IEEE INFOCOM, 2010.

[9] B. B. Romdhanne, D. Dujovne, and T. Turletti, “Efficient and scalable merging algorithms for wireless traces,” in Workshop on Real Overlays and Distributed Systems (ROADS), Oct. 2009, pp. 1–7.

[10] A. Balachandran, G. M. Voelker, P. Bahl, and P. V. Rangan, “Characterizing user behavior and network performance in a public wireless LAN,” in ACM SIGMETRICS, Jun.15-19 2002, pp. 195–205.

[11] M. Sammarco, M. E. M. Campista, and M. D. de Amorim, “Trace selection for improved WLAN monitoring,” in ACM HotPlanet Workshop, Aug.16 2013, pp. 1–6.

[12] M. E. J. Newman and M. Girvan, “Finding and evaluating community structure in networks,” Physical Review E, vol. 69, no. 2, pp. 026 113+, Feb. 2004.