International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 04 Issue: 11 | Nov -2020 ISSN: 2582-3930

Secure and Efficient Data Transmission in Cluster based Wireless Sensor Network with RSA Algorithm

Sugunamuki.K.R
Computer Science
Sri Shakthi Institue Of Engineering And Technology,
Coimbatore

S.Hemalatha
Assistant professor
Computer Science
Sri Shakthi Institute Engineering and Technology,
Coimbatore,

Abstract - **Wireless Sensor Network (WSN) is a collection of nodes which are deployed in an environment where the data is needed to be sensed to monitor any changes in surrounding. Each nodes are equipped with memory, battery, transceivers. The nodes are placed in such an environment where monitoring by human is difficult to schedule or managed efficiently by individual. Each node is responsible for manipulating the data it has sensed and transferring it to the base station (BS). These nodes are grouped into clusters so that the drainage of battery in wireless sensor Network can be overcome and increase the scalability. In each cluster there is a cluster head (CH) which acts as a leader of the cluster and is responsible for gathering all the manipulated data from the each nodes in the cluster and transferring it to the base station. There is a need of secure and efficient transmission of data in cluster based WSN (CWSN) which will be discussed. The existing method uses genetic leach to make energy efficiency in sensor Network. We have proposed a protocol called CBSRP which mainly focuses on the security of the data to be transmitted and confidentiality of data is provided through RSA algorithm, a well known cryptographic technique for secure datatransmission.**

Keywords: Wireless Sensor Networks, Energy Consumption, Sensors, Monitoring, Optimization, Energy Conservation

I INTRODUCTION

The structuring of a Network is one of the main tools to save energy in each Network node. In sensor Networks there are two types of architecture for Networks, flat architecture that constitutes a homogeneous Networkwhere all nodes have the energy resources, calculation and memory, and another hierarchical.

Architecture where all nodes do not have the same roles and therefore the same resources. Being given that the main purpose of a routing protocol for WSN is the proper and efficient development of routes between a pair of nodes so that messages can be routed, why multiple routing protocols (hierarchical protocols, flat protocols) have been developed these last year's.

The comparison studied between the flat and hierarchical structure at the energy consumption level shows that the hierarchical architecture has more advantage than the flat architecture, namely: well-structured Network, easy Network management, less power consumption, high lifetime, unless the message circulating on Networks and the flood problem isavoided.

In the other hierarchical structure there are two main approaches are derived from these protocols: cluster-based approach and chain–based approach:

1.Cluster-based approach: the node is organized in cluster, each cluster have his leader to transmit a data to the base station.

Genetic Algorithm Based Improvisation of LEACH protocol

same in terms

2. Chain–based approach: the node is organized in a chain to send the data to the basestation.

Dynamic source routing will ISA basic also productive directing protocol planned for a chance to be utilized to portable hubs done multi-jump remote Adhoc Networks. It supports two different tables similar to course discovery, course maintainer. Temporally ordered routing algorithm is awful adaptive, bend-free, and analysis acquisition algorthimis absolutely based on the abstraction of articulation abortion and reversal.

Particulation abortion and reversal. Synchronous alarm is appropriate for antecedent accomplished action and provides assorted routes for the antecedent to destination pair. This agreement maintains three phases 1) route creation, 2) route maintenance and 3) route elimination. Associatively basedroutings.

Mobile routing protocol which is introduced to find the stable links among the nodes while keys for that node should free from the duplicate key and it performs retransmission process also. Hybrid routing may be a directing protocol that combines both proactive and sensitive routing; it might have been suggested to decrease the control overhead about proactive directing also likewise declines those inactivity brought about toward course finding in the sensitive directing protocol. Mixture directing protocol would ZRP also TORA. Zone directing protocol might have been arranged to decrease those control through leader for proactive directing also decline those inactivity created eventually tom's perusing thosecourse

II OBJECTIVE

In WSN, both clustering and secure route detection enhance efficiency in routing. Stability and reliability of cluster-based approach depend on quality of cluster head and gateway nodes. Cluster formation and secure route detection play inevitable roles in WSN. Thus motivation of CBSRP is:

1. Cluster formation and selection of stable, reliable cluster heads to reduce routing overheads.
2. Detection of a secure set of routes in the cluster based environment and selecting the final secure route containing nodes with the highest weight values to reach thedestination

III EXISTINGSYSTEM

The structuring of a Network is one of the main tools to save energy in each Network node. Energy can be efficiently used up to some level in one of the hierarchy routing protocol that is Low Energy Adaptive Clustering Hierarchy (LEACH). LEACH protocol is based on grouping techniques and also efficient routing protocol for WSN. The nodes in the Network area of LEACH are considered as local clusters. Genetic Algorithm Based Improvisation of LEACH protocol.

optimized using Genetic Algorithm (GA) to extend the life time of WSN. Genetic LEACH increases the living time of the WSN compared withLEACH,andalsotheinterclustercommunicationin LEACH reduces energy consumption by the nodes significantly and the living period of WSN is increased compared with LEACH and with Genetic LEACH.

3.1 Disadvantages:

1. Security consideration on the data transmission is notmade.
2. Optimal method of increased energy efficiency is given whereas, Network overhead is notsatisfied.

IV PROPOSEDSYSTEM

A WSN is a special type of Network. It shares some commonalities with a typical computer Network, but also exhibits many characteristics which are unique to it. The security services in a WSN should protect the information communicated over the Network. Routing overheads and security are the main challenges of Wireless Sensor Network. The idea behind clustering is to group Network nodes into a number of disjoint or overlapping clusters. Cluster-heads of the clusters take an active role in routing messages between a source destination pair. The Proposed work is the implementation of an efficient protocol CBSRP (Cluster Based Secure Routing Protocol) which is a cluster based approach to decrease the routing overheads as CBSRP elects most reliable and stable node as cluster head and concerns on secure data transmission applying Shamir's secret sharing method. For message encryption and decryption the proposed protocol uses RSA- CRT algorithm. In this CBSRP Confidentiality of the transmitted data is maintained by encrypting the data with RSA. Mitigation of all the other security threats like packet loss or loss of data integrity is achieved by detecting the secure set of routes and finding the final secure route with highest average weightvalue.

4.1Advantages:

1. RSA implementation provides secure data transmission among the clusternodes.
2. Stable and reliable clusterformation.
3. Routing overhead is greatlyreduced.

V FEASIBILITYSTUDY

The problem is clearly understood and solutions are proposed accordingly, feasibility study has been done, which is a part of the system analysis as well as system design process. The main objective of this study is to determine whether the proposed system is feasible or not. And feasibility is the measurement of how suitable the development of a system will be to the user. There arethreeaspects in the feasibility portion of the preliminary investigation.

1. Technicalfeasibility
2. Economicfeasibility
3. Operationalfeasibility
4. Socialfeasibility

5.1 Technicalfeasibility

Technical feasibility investigates whether the project can be developed with the hardware as well as software requirements. The considerations those are normally associated with technical feasibility are development risk, resource availability and technology. Running the application in the device first time requires plug-in, and not required for subsequent usages, and it also does not overload the device memory. Therefore our application tends to be feasibletechnically.

5.2 Economicalfeasibility

Feasibility studies are crucial during the early development of any project and form a vital component in the business development process. Accounting and advisory feasibility studies enable organizations to assess the viability, cost and benefits of projects before financial resources are allocated. They also provide independent project assessment and enhance projectcredibility.

Built on the information provided in the feasibility study, a business case is used to convince the audience that a particular project should be implemented. It is often a prerequisite for any funding approval. The business case will detail the reasons why a particular project should be prioritized higher than others. It will also sum up the strengths, weakness and validity of assumptions as well as assessing the financial and non-financial costs and benefits underlying preferred options. We can implement this project with low cost because we are using .NET. It can be more economically feasible.

5.3Operationalfeasibility

Operational feasibility is a measure of howwella theopportunitiesidentifiedduringscopedefinitionand how it satisfies the requirements identifiedinthe requirements analysis phase of the system development.

The operational feasibility assessment focuses on the degree to which the proposed development projects fits in with the existing business environment and objectives with regard to development schedule, delivery date,corporate culture, and existing business processes. To ensure success, desired operational outcomes must be imparted during design and development. These include such design-dependent parameters such as reliability, maintainability, supportability, usability, productivity, disposability, sustainability, affordability and others. These parameters are required to be considered at the early stages of design if desired operational behaviors are to be realized. A system design and development requires work appropriate and timely application of engineering and management efforts to meet the previously mentioned parameters. A system may serve its intended purpose most effectively when its technical and operating characteristics are engineered into the design. Therefore operational feasibility is a critical aspect of systems engineering that needs to be an integral part of the early designphases.

5.4 Socialfeasibility

The aspect of study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system, instead must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make him familiar with it. His level of confidence must be raised so that he is also able to make some constructive criticism, which is welcomed, as he is the final user of thesystem.

VI SYSTEMREQUIREMENTS

6.1 HardwareRequirements

This section gives the details and specification of the hardware on which the system is expected to work.

Processor	:	IntelPentium
Hard Disk	:	60 GB
Monitor	:	VGAColor
RAM:	:	512 MB

proposedsystemsolvestheproblems,andtakesadvantage of

6.2 Softwarerequirements

This section gives the details and specification of the software on which the system is expected to.

FrontEnd/GUI Tool : Microsoft Visual studio .NET

OperatingSystem : Windows07

Language : VB.NET / C#.NET
Application : DesktopApplication

BackEnd : MSACCESS

6.3Softwaredescription

6.3.1.NETframework

The .NET framework has two main parts:

- Common language runtime(CLR)
- Hierarchical set of classlibraries

The CLR is described as the "execution engine" of .NET. It provides the environment within which programs run. The most important features are,

1. Conversion from a low-level assembler –style language, called intermediate language (il), into code native to the platform being executedon.
2. Memory management, notably including garbage collection.
3. Checking and enforcing security restrictions on the runningcode.
4. Loading and executing programs, with version control and other suchfeatures.

The following features of the .NET framework are also worth description:

Managed code

The code that targets .NET, and which contains certain extra information - "metadata" - to describe itself. Whilst both managed and unmanaged code can run in the runtime, only managed code contains the information that allows the CLR to guarantee, for instance, safe execution and interoperability.

Managed data

With managed code comes managed data. CLR provides memory allocation and deal location facilities, and garbage namely C++, do not. Targeting CLR can, depending on the language you're using, impose certain constraints on the features available. As with managed and unmanaged code, one can have both managed and unmanaged data in.NET.

Common type system

The CLR uses something called the common type system (CTS) to strictly enforce type-safety. This ensures that all classes are compatible with each other, by describing types in a common way. CTS defineshow types work within the runtime, which enables types in one language to interoperate with types in another language, including cross – language exception handling. As well as ensuring that types are only used in appropriate ways, the runtime also ensures that code doesn't attempt to access memory that hasn't been allocated to it.

Common language specification

The CLR provides built-in support for language interoperability. To ensure that you can develop managed code that can be fully used by developers using any programming language, a set of language features and rules for using them called the common language specification (CLS) has been defined. Components that follow these rules and expose only CLS features are considered CLS- compliant.

The class library

.NET provides a single – rooted hierarchy of classes, containing over 7000 types. The root of the namespace is called system. This contains basic types like Byte, Double, Boolean and String, as well as object. All objects derive from system. Object, as well as objects, there are value types. Value types can be allocated on the stack, which can provide useful flexibility. There are also efficient means of converting value types to object types if and when necessary.

The set of classes is pretty comprehensive, providing collections, file, screen, and Network i/o, threading, and so on, as well as xml and database connectivity.

The class library is subdivided into a number of sets (or namespaces), each providing distinct areas of functionality, with dependencies between the namespaces kept to a minimum.

collection. Some .NET languages use managed data by default, such as C#, Visual Basic.NET and Jscript.NET, whereas others,

Language support by .NET

The multi-language capability of the .NET framework and visual studio .NET enables developers to use their existing programming skills to build all types of applications and xml web services. The .NET framework supports new versions of Microsoft's old favorites visual basic and C++ (as vb.NET and managed C++), but there are also a number of new additions to thefamily.

Visual basic .NET has been updated to include many new and improved language features that make it a powerful object-oriented programming language. These features include inheritance, interfaces, and overloading, among others. Visual basic also now supports structured exception handling, custom attributes and also support multi-threading.

C# is Microsoft's new language. It's a c-style language that is essentially "C++ for rapid application development". Unlike other languages, its specification is just the grammar of the language. It has no standard library of its own, and instead has been designed with the intention of using the .NET libraries as it own.

Other languages for which .NET compilers are available include

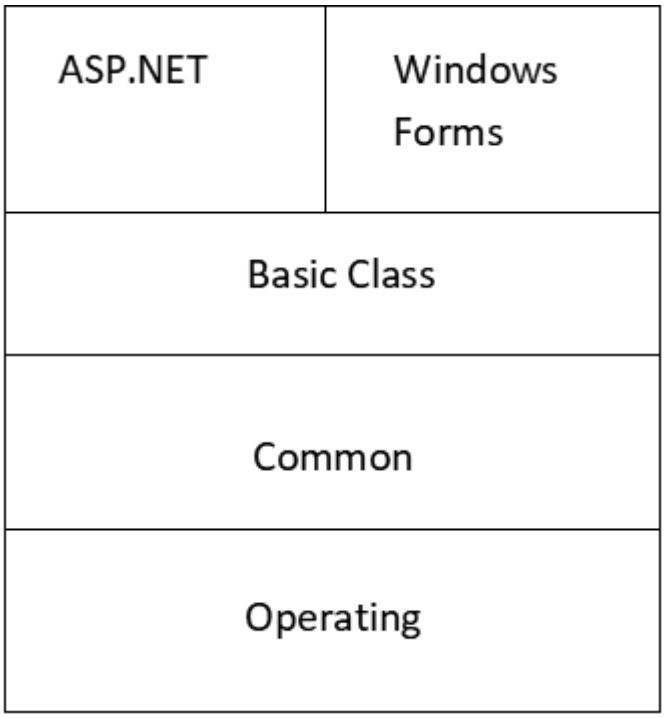
a. Fortran
b. Cobol
c. Eiffel

Visual basic .NET, the next generation of the visual basic language, is a fast and easy way to create .NET-based applications, including xml web services and web applications.

Visual basic .NET has many new and improved features that make it a powerful object-oriented programming language, including inheritance, interfaces, and overloading. Other new language features include free threadingandstructuredexceptionhandling.Visualbasic

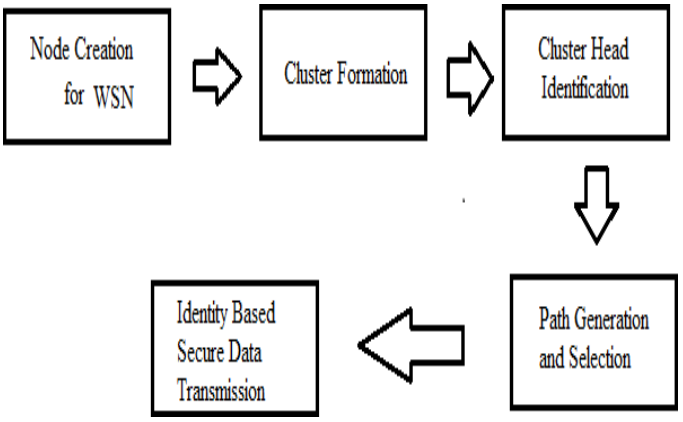
.NET also fully integrates the .NET framework and the common language runtime, which provide language interoperability, garbage collection, enhanced security, and improved versioning support.

Vb.NET is a CLS-compliant langue. Any objects, classes, or components that created in vb.NET can be used in any other CLS-compliant language. In addition, we can use objects, classes,



VII SYSTEMDESIGN

7.1 Architecture diagram



and components created in other CLS- compliant languages in vb.NET. The use of CLS ensures completeinteroperability

VIIISYSTEMDEVELOPMENT

CBSRP

Cluster based Network is considered. Here two clusters have been formed with different number of nodes. Each cluster have leader to transmit a data to the base station. The leader of the cluster is called cluster head. The efficiency of the cluster based Network relies mainly on the cluster head selection. Cluster-heads of the clusters take an active role in routing messages between a source destination pair. The cluster formation and the cluster head selection is made by using CBSRP (cluster based secure routing protocol). CBSRP elects most reliable and stable node as clusterhead.

RSA

RSA makes use of an expression with exponentials.
Plaintext is encrypted in blocks, with each block having a binary value less than some integer n.Encryption and decryption are of the following form, for some plaintext block M and cipher text block C:

$$C = M^e \bmod n$$

$$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$$

Both sender and receiver must know the value of n. The sender knows the value of e, and only receiver knows the value of d. Thus, this is a public-key encryption algorithm with a public key of KU={e,n}, and a private key of KR={d,n}.

For this algorithm to be satisfactory for public- key encryption, the following requirements must be met:

1. Itispossibletofindvaluesofe,d,nsuchthat for all M<n
2. It is relatively easy to calculate M^e and C^d for all values of M<n
3. It is infeasible to determine d given e andd.

A corollary to Euler's theorem For every a and n that are relatively prime

$$a^{\varphi(n)} \equiv 1 \bmod n$$

following relationship holds:

$$m^{k\varphi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$$

(as far as for p,q prime, $\varphi(n) = (p-1)(q-1)$)

Thus, we can achieve the desired relationship if $ed = k\varphi(n) + 1$

This is equivalent to saying:

$$ed \equiv 1 \bmod \varphi(n)$$
$$d \equiv e \bmod \varphi(n)$$

e and daremultiplicativeinverses $\bmod \varphi(n)$
Note that, according to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to $\varphi(n)$.

Equivalently,

$$\gcd(\varphi(n), d) = 1$$

We are now ready to state the RSA scheme. The ingredients are the following:

n=pqp ,q, twoprimenumbers

$\gcd(\varphi(n), e) = 1; 1 < e < \varphi(n)$ (public, chosen)

$d \equiv e^{-1} \bmod \varphi(n)$ (private, calculated)

The private key consists of {d,n}, and the public key consists of {e,n}. Suppose that user A has published its public key and that user B wishes to send message M to A.

Then B calculates $C = M^e \bmod n$and transmits C. On receipt of this cipher text, user A decrypts by calculating $M = C^d \bmod n$

It is worthwhile to summarize the justification for this algorithm.Wehavechoseneanddsuchthat

$d \equiv e^{-1} \bmod \varphi(n)$

Therefore, ed is of the form $k\varphi(n) + 1$. But by the

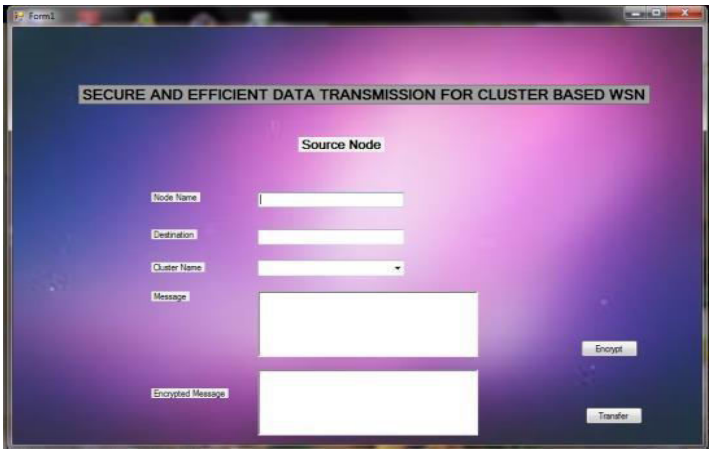
where $\varphi(n)$ is the Euler's totient function – number of positive integers less than n and relatively prime to n

Given two prime numbers, p and q two interger n and m, such that n=pq and 0<m<n, and arbitrary integer k, the

Now, $C = M^{e} \bmod n$

$M = C^{d} \bmod n \equiv (M^{e})^{d} \bmod n \equiv M^{ed} \bmod n \equiv M \bmod n$

IX SCREENSHOTS



X REFERENCES

[1] R.Sujee, Dr.Kannammal, "Energy Efficient Adaptive Clustering Protocol Based on Genetic Algorithm and Genetic AlgorithmInterCluster Communication for Wireless Sensor Networks", 2017 International Conference on Computer Communication and Informatics (ICCCI - 2017), IEEE2017

[2] Hassan Oudani, SalahddineKrit, Mustapha Kabrane, KaoutarBandaoud, Mohamed Elaskri, Khaoula Karimi, Hicham Elbousty, LahoucineElmaimouni, "Energy Efficient in Wireless Sensor Networks Using Cluster- Based ApproachRouting"

[3] Jaydip Sen "Security in Wireless SensorNetworks"

[4] Reza Azarderakhsh, ArashReyhani-Masoleh, and Zine- Eddine Abid, "A Key Management Scheme for Cluster Based Wireless corollary to Euler's theorem (*), given two prime numbers, p and q, and integer n=pq and M, with 0<M<n:

$$M^{k\varphi(n)+1} = M^{k(p-1)(q-1)+1} \equiv M \bmod n$$

[5] Rajwinder Kaur, Sandeep Singh Kang, "A Secure Packet Handover Scheme using RSA Algorithm in WirelessNetworks"

[6] V.Saravanan, R.Rajkumar, "Secure Source-Based Loose RSA Encryption for Synchronization (SSOBRSAS) and Evolutionary Clustering Based Energy Estimation for Wireless Sensor Networks", International Journal of Advanced Research in Computer Science, June2014

[7] Sandhyarani B H, NagnathBiradar ,T.S.Vishwanath, "An Authenticative Way To Data Transmission For Cluster Based Wireless Sensor Network", IJRET: International Journal of Research in Engineering and Technology eISSN: 2319-1163 | pISSN:2321-7308,May 2015

[8] Sohini Roy, Diptipriyasinha, "Cluster Based Secure Routing Protocol", IEEE2014

[9] Z. Yu and Y. Guan, "A dynamic en-route scheme for filtering false data injection in wireless sensor networks," *Proc. of IEEE INFOCOM*, pp. 1–12, April 2006.

[10] F. Ye, H. Luo, S. Lu, and L. Zhang, "Statistical en-route filtering of injected false data in sensor networks," *IEEE JSAC*, vol. 23, no. 4, pp. 839–850, April 2005.