Secure Multicasting using Geographical Information: A Cluster Based Approach in Wireless Sensor Networks

Manjunath C R[1], Sindhu Anand[2]
[1,2] Department of Computer Science and Engineering
School of Engineering and Technology
Jain University

Abstract:- **In order to guarantee the privacy and safety of data transactions in Wireless Sensor Networks, secure key transportation and unique node identification have become major concerns. WSNs are deployed in a wide range of applications with a high demand for secure communications. When designing a secure key management for a secure communication channel establishment in WSNs, attention should be given to the resource constraints of the devices and the scalability of the network. Here an attempt for public-key to define a hybrid key establishment algorithm for symmetric key cryptography. An Elliptic Curve Cryptography based implicit certificate scheme and how to utilize the certificates for deriving pair-wise link keys in a WSN, by a performance and security analysis. A new approach for secure communication channel establishment is made in order to suite the functional and architectural features of WSNs.**

Keywords: Wireless Sensor Networks, certificate, secure communication, key establishment, Elliptic Curve Cryptography.

I. INTRODUCTION:

Wireless Sensor Networks [3][4][5][14][16] (WSN's) applications are used in various fields from commercial and industrial to military areas. There is a need for security in WSNs, as they communicate happens in an insecure communication medium and they often operate unattended. These devices are economically viable; they have a limited amount of energy, computation power, and memory and communication abilities. A node's lifetime is influenced by the amount of energy that it uses to perform computations and is therefore it's directly influenced by the efficiency of its algorithms. A Pairwise keying process provides basic security services in wireless sensor networks. That enables sensor nodes to communicate securely with each other using cryptographic techniques. Typical public-key cryptography is a low-power domain is for Wireless Sensor Network. The data is transmitted towards the base station using single-hop connectivity comprising of wireless communication links with the nodes, where the data need to be sent in a secure manner. Encryption algorithms for secure transmission are make use of complex algorithm without the key it's impossible to extract information through a cryptanalysis. The classes of cryptographic algorithms can be classified as symmetric or asymmetric. Greater robustness against sensor node does come at a cost, particularly in the overhead involved for key management. If a sensor node communicates with a large number of nodes, it will and must store many keys and select the appropriate ones when communicating. Wireless sensor network in which the nodes are deterministic with similar computational and communication capabilities. The network uses Clustering technique for key distribution and secure communication. In a cluster, all the nodes maintain different keys, but every node uses same key for different communications with the base station.

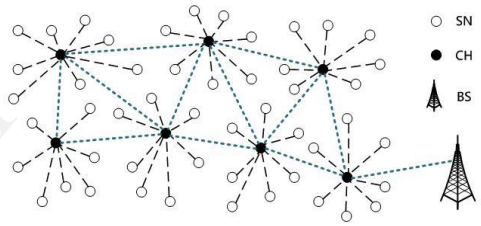

Fig 1: General Architecture of the Network

WSN [15] architecture with cluster is based on different topologies which can be established for heterogeneous and homogeneous networks. The topology in every type of data collecting and monitoring WSNs, there is a cluster head or a network coordinator node. The nodes are deployed in predefined clusters under the control of particular CH. Generally, the CH acts as the intermediate coordinator between sensors and the base station. Sensor nodes gather data from their corresponding area and send data to CH or the base station via single hop or multi-hops. The communication links are very short-term and dynamic changing. For such pair-wise link keys are required for secure communication since symmetric key encryption is more cost effective

II. RELATED WORK / LITERATURE SURVEY:

Key management has remained a challenging issue in WSNs due to the constraints of sensor node resources. Various key management schemes that trade off security and operational requirements have been proposed in recent years.

i. Xiaowang Guo, Jianyong Zhu: [1] has addressed the most suitable asymmetric cryptography primitives for WSN, the Elliptic Curve Cryptography cryptosystem security based on the discrete logarithm problem, and the main ECC primitive operation is the scalar point multiplication.

ii. Ahmad Salehi S, M.A. Razzaque, Parisa Naraei, Ali Farrokhtala: [2] addresses the issues in straight pairwise key participating amongst each two nodes in a large network which have many nodes since. Here an effective key distribution technique in found for preserving the capability to communicate among all related nodes.

iii. Bin Tian, Kamal Kant M. R. Tripathy: [5] addresses about a hierarchical key management scheme to ensure the security of the network services and applications and how it can save the computing and transmitting energy for large-scaled WSNs

III. KEY MANAGEMENT AND KEY DISTRIBUTION:

Key [1] [11] management is one of the most important issues of any secure communication. With the increasing demand for the transmission security in wireless sensor networks, the key management can be done in two methods, providing session key to individual nodes and providing key management to group nodes, before exchanging data securely, encryption keys must be established among sensor nodes. Key usage for secure data transmission, it does not specify how to exchange keys securely. Besides the link layer, upper layers such as the network and application layers also must exchange keys securely. This is a challenging problem because there are many stringent requirements for key management, and the resources available to implement such processes are highly constrained. Many security-critical applications depend on key management processes to operate but also demand a high level of fault tolerance. Multiple Keys are distributed among the sensor nodes; each node must broadcast the key's ID within its communication range to find out if the nodes share the same key. A secure communication can be established as long as there is at least one key being shared. If there is no key shared between two nodes, then the link has to be established through two or more paths.

IV. SECURE TRANSMISSION IN WSN: KEY DISTRIBUTION SCHEMES

There are [11] three keying models that are compared between the WSN security and operational requirements which are network keying, pairwise keying, and group keying. The network keying model has advantages over the pairwise keying, and group keying. It is simple, easy to manage, and uses very little resources. It allows collaboration of nodes where neighbouring nodes can read and interpret each other's data, it is self-organizing, scalability and accessible. The drawback of network keying is robustness.

The pairwise keying it is difficult to add new nodes to the network, hence affecting the flexibility requirement. This is a resource-intensive process that uses more energy when compared with the simple preloading of a network-wide key as in the network keying. Some pairwise key distribution are self-organization, because they tackle the scalability problem by reducing the number of shared keys, results in some nodes being unable to communicate with other nodes and hence compromising the self-healing and self-organizing abilities of the network.

The group keying combines the features of both network and pairwise keying techniques. When group of nodes form a cluster, communications are performed using a single, shared key similar to network keying. The communications between group's uses a different key between each pair of groups in a manner identical to the pairwise keying technique. Scalability, increase keys with the number of groups, not with the size of the network. The drawback with this technique is that it is difficult to set up and also the formation of the groups is a very application dependent.

A. Elliptic Curve Cryptography:

Elliptic curve cryptography [1][8] (ECC) is used for a efficient implementation of a public-key cryptography algorithm, where the security is achieved by using key encryption and decryption to solve the discrete logarithm problem. Most of the Public key cryptography systems are designed based on the RSA algorithm but reaches prefer ECC, because it provides same level of security with much smaller key size and both the public key and private key operation use the same point multiplication operations unlike RSA.

ECC is based on elliptic curves the variables and coefficients which are limited to the elements in a finite field. The finite field is classified by the sizes which are exactly one finite field up to isomorphism of size p^n for each prime p and positive integer n. The elliptic curve in the finite field F_p is a prime curve if p is a prime number, and F_p is defined as a set of integers{0,1,..., p-1}. The elliptic curve is a binary curve in the finite field F_2^m, where m is a large integer andF_2^m is defined as a set of integers {0, 1,..., 2n-1}.

The prime field is Fp. An elliptic curve E is expressed by the equation $y^2 = x^3+ax+b$. The elliptic curve E is defined in the prime field F_p, where the point (x, y) falling into the elliptic curve E will meet the equation

$y^2 = x^3+ax+b(\text{mod } p)$ …… (1)

The above equation is expressed as $E_p(a,b)$, where p is a large prime number and x, y, a, b are the elements of the finite field F_p. Also, a and b must satisfy the following equation

$4a^3 + 27b^2 (\text{mod } p) \neq 0$…….. (2)

B. Diffie Hellman Key Exchange:

The Diffie-Hellman [6][7] key exchange method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. The key value is used to encrypt subsequent data using a symmetric key cipher. The interpretation of the data packets for verification is performed only when the nodes pass the Diffie Hellman key exchange mechanism, for every non-leaf node is labelled with the its children nodes.

Diffie-Hellman Key Exchange Algorithm

1. Public key, Parameter Creation. A Cluster head chooses and publishes a Prime Public key P and a key c having large prime order in C^*_R.
2. Private key Computations, Node A Choose a secret key a and Compute Node A ≡ c^a (mod P). Node B Choose a secret key b and Compute Node B ≡ c^b (mod P).

3. Public key Exchange of key values
   Node A sends A to Node B → A
   B ← Node B sends B to Node B
4. Further Private key Computations Node A Compute the key value B^a (mod P). Node B Compute the key value A^b (mod P).
5. The shared secret key value is $B^a = (c^b)^a = c^{ab} = (c^a)^b = A^b$ (mod P).

Final key without sharing each other's private random number and c sitting in between will not be able to determine the key as the private numbers were never transferred. The Diffie-Hellman algorithm works perfectly to generate cryptographic keys which are used to encrypt the data being communicated over a public channel.

C. Certificate Generation Method:

A WSN consists of hundreds or thousands of densely populated sensor nodes spread over a medium scaled network, which sense the data and propagate through the network. They work collaboratively to process and sensed data. These sensor nodes send data streams to base stations either periodically or based on events and base station send the data to the destination node. In a network, sensors nodes may be densely populated wit, the area detected by the sensors are dividing into a number of small clusters.

A Grid is a cluster based schemes, in which clusters are equally sized square grids in a two dimensional plane, have a simple structure with less routing management overhead. With the assistance of GPS or localization techniques, the square grid also provides easier coordination among all sensor nodes in the network.

The base station plays a major role in forming the secure transmission channel which acts like a gateway for external communication. The base station gathers information of all the nodes from the Grid to form the clusters according to the location of the nodes. A key management mechanism is used which is based on ECC. It provides authentication services for the identity of nodes and message transmission between the source and destination. It provides a mechanism the add nodes with pre-loaded public keys as certificates to help the other nodes verify their trust worthiness. By doing so, the old nodes do not have to update their keys for secure communications with the new nodes.

Algorithm get Certificate () {
  Every node in the sink node transmission region {
    Request for certificate
    If its valid Authenticated request then
   Certificate Authentication or the Base Station grants certificate to node
    Node gets the certificate}}

Using this algorithm every node in sink transmission range need to ask the permission i.e. certificate from Certificate Authentication to communicate other nodes within its transmission range. The sink node check their authentication if it is valid it grants a certificate to the node otherwise rejected.

Algorithm for send message (){
  If (cluster head sends message to other head) {
    If (sending node is checked for their validation) {
      Message is accepted to receive or route}
  Reject the message}

If any node or header node want to send some information to other header node in the cluster they need to prove their validation based on certificate.

During the node deployment, each sensor node has to go through an initialization phase, where the base station certifies the trust worthiness of the nodes. The base station generates a pair of public and private keys for each node that issues pre-loaded certificates to ensure the trust worthiness of the newly added nodes. Pre-loaded public key can be used as the certificate to ensure the trust worthiness of the newly added nodes to the network. The nodes within a cluster can verify their trust worthiness with each other within the valid period of certificates generation

V. DIFFERENT KEY MANAGEMENT APPROACH:

Key Distribution Approach	Key used
Random	The size of the key ring cannot be small
Deterministic	Graph based stores a key ring. Grid based stores k- dimension key management
Location Based	The location information and direct key is added
Key Agreement Model	Link Compromise Probability
Predistributed keys	approximately linear or quickly increasing to number of compromised nodes
matrices or polynomials	threshold-based
Key Material Deployment Pattern	Local Secure Connectivity
Uniform	Low
Location - based	High

VI. PROPOSED SCHEME:

An attempt is made to provide a secure communication channel for WSN. There are several issues that restrict the network in terms of providing security and managing the network. The key management technique helps to overcome such issues. A grid based network is used the make the network manageable and reduce the computation time while accessing the node. A hybrid cryptography scheme is proposed, where the ECC and DH are combined with a certificate added to the cluster head.

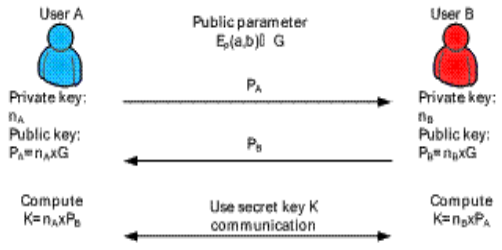

Fig 2: Key Exchange Mechanism.

A. Hybrid Cryptography:

Symmetric [9]key algorithm has a disadvantage of key distribution and asymmetric algorithm need much computation so the power of the sensor is wasted in it and it is not feasible to use as power is wasted then sensor will be of no use. A hybrid cryptosystem is a protocol using multiple ciphers of different types together, each to its best advantage. One common approach is to generate a random

secret key for a symmetric cipher, and then encrypt this key via an asymmetric cipher using the recipient's public key. The message itself is then encrypted using the symmetric cipher and the secret key. Both the encrypted secret key and the encrypted message are then sent to the recipient. The recipient decrypts the secret key first, using his/her own private key, and then uses that key to decrypt the message. The certificate is generated and added to hybrid key management, with ECC+DH. By using this certificate it makes the cluster more secure.

VII. RESULT AND ANALYSIS:

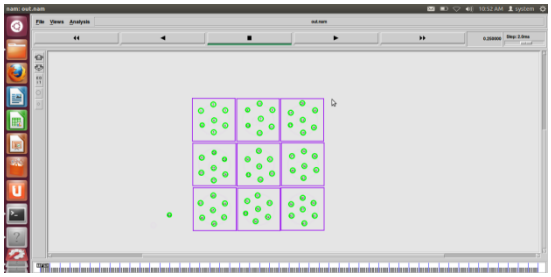

Fig 3: Node deployment.

Node deployment is made deterministic and grids are formed with clusters inside each grid. A cluster head is assigned to each cluster and a Base Station to monitor all the cluster heads as shown in Fig 3.

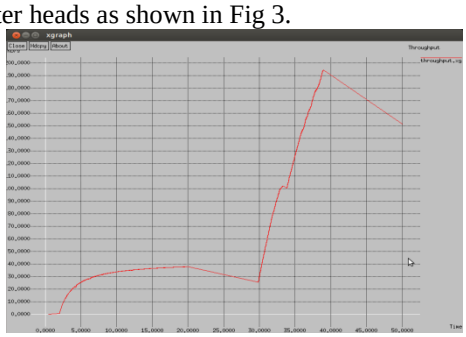

Fig 4: Throughput Graph

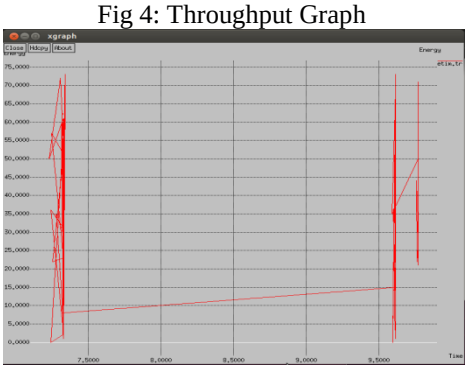

Fig 5: Energy Efficiency Graph

Fig 6: Packet Delivery Ratio.

The proposed system utilizes the energy of the node efficiently, the packet delivery ratio is high and stays moderate due to which the energy consumption is limited. The throughput is high is and hence there is a faster delivery of the data in the network.

VIII. Conclusion:

An attempt as been made to introduced a certificate based pairwise key establishment protocol for WSNs. The proposed key management scheme comprises two phases: For providing certificates for the nodes and establishing pairwise link keys for mutual communication node between the nodes. A secure Public Key Cryptography based solution is derived for a common secret key for symmetric key encryption. The novelty is the utilization of implicit certificates for generating pairwise keys. Our experimental results show the feasibility of deploying the proposed scheme in an actual resource constrained WSN. However, the further optimized ECC operations may have less resource consumptions on sensor nodes and accelerate the protocol execution. Moreover, we have discussed and justified the appropriateness of the protocol for the resource utilization and scalability of WSN. Though there is a simple concept behind the proposed scheme, the security analysis has proven the robustness of the protocol for different security. In future, we intend to extend this protocol by changing the content of the certificate in such way to provide higher security for mobile sensor nodes in massive scale networks. We can customize the content of the implicit certificates by adding other information such as the time stamp, location identity, depending upon the application requirements. The certificates are utilized for group key management in large scale sensor networks.

REFERENCES:

[1]. Cheng-Lung Yang[1], Wernhuar Tarng, Kuen-Rong Hsieh and Mingteh Chen A Security Mechanism for Clustered Wireless Sensor Networks Based on Elliptic Curve Cryptography IEEE 2010.

[2]. Ruan de Clercq, Leif Uhsadel, Anthony Van Herrewege, Ingrid Verbauwhede K.U. Leuven Ultra Low-Power implementation of ECC on the ARM Cortex-M0+, Department of Electrical Engineering and iMinds Kasteelpark Arenberg 10, 3001 Heverlee-Leuven, Leuven, Belgium.

[3]. Gustavo S. Quirino, Admilson R. L. Ribeiro and Edward David Moreno Asymmetric Encryption in Wireless Sensor Networks INTECH 2012.

[4]. Ismail Butun and Ravi Sankar A Brief Survey of Access Control in Wireless Sensor Network IEEE 2010.

[5]. Mohamed Hamdy Eldefrawy1, Muhammad Khurram Khan1, Khaled Alghathbar A Key Agreement Algorithm with Rekeying for Wireless Sensor Networks using Public Key Cryptography. IEEE 2010.

[6]. Geetha, Jayalakshmi Performance Analysis of Sdrp for Wsn Using Diffie – Hellman Algorithm IOSR Journal of Computer Engineering Volume 16, Issue 2, Ver. XII (Mar-Apr. 2014), PP 19-23.

[7]. R.Dhanalakshmi K.Pradeepa Improved Key Selection Techniques for Wireless Sensor Networks IJSR - INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH volume:3 Issue: 4 April 2014.

[8]. Pritam Gajkumar Shah, Xu Huang, Dharmendra Sharma, Analytical study of implementation issues of Elliptical Curve Cryptography for Wireless Sensor networks International Conference on Advanced Information Networking and Applications Workshops IEEE 24th 2010.

[9]. Madhumita Panda Security in Wireless Sensor Networks using Cryptographic American Journal of Engineering Research (AJER) e-ISSN : 2320-0847 p-ISSN : 2320-0936 Volume-03, Issue-01, pp-50-56 2014.

[10]. Srikanta Kumar Sahoo and Manmanth Narayan Sahoo An Elliptic Curve based Hierarchical Cluster Key Management in Wireless Sensor Network 2010.
[11]. Pratik Ranjan Nachiketa Tarasia An Efficient Node Authentication Scheme based on Elliptic Curve Cryptography for Wireless Sensor Networks (IJCSET) ISSN: 2229-3345 Vol. 4 No. 05 May 2013.
[12]. Mr. G. Ravi, Mr. M. Mohamed Surputheen & Dr. R. Srinivasan Fast Energy-Efficient Secure Dynamic Address Routing For Scalable WSNs IJCSI International Journal of Computer Science Issues, Vol. 9, Issue 2, No 1, March 2012.
[13]. Xu Huang, Pritam Shah, and Dharmendra Sharma Fast Algorithm in ECC for Wireless Sensor Network VOL II IMECS 2010 March 17-19, 2010.
[14]. Shantala Devi Patil, Vijayakumar B P A Public key distribution and Broadcast Authentication scheme for Wireless Sensor Networks International Conference on Recent Development in Engineering and Technology, 5th August , Mysore,ISBN-978-93-82208-00-6.
[15]. Pawani Porambage, Pardeep Kumar, Corinna Schmitty, Andrei Gurtovz and Mika Ylianttila Certificate-Based Pairwise Key Establishment Protocol for Wireless Sensor Networks 2010.
[16]. A.Ramakrisha , P.VijayaBharathi Secured Dynamic Routing Strategy in Wireless Sensor Networks International Journal of Scientific & Engineering Research, Volume 4, Issue 7, July-2013 179 ISSN 2229-5518.
[17]. Huang Lu, Student Member, Jie Li, Senior Member, Mohsen Guizani, Secure and Efficient Data Transmission for Cluster-based Wireless Sensor Networks, IEEE Transactions On Parallel And Distributed System Year 2013.
[18]. Gicheol Wang, and Gihwan Cho Securing Cluster Formation and Cluster Head Elections in Wireless Sensor Networks International Journal of Communication Networks and Information Security (IJCNIS) Vol. 6, No. 1, April 2014.
[19]. Andrey Khurri, Dmitriy Kuptsov, and Andrei Gurtov On Application of Host Identity Protocol in Wireless Sensor Networks2010