Optimized Routing and Trust Based Data Dissemination in Wireless Sensor Networks

Shahanaz.S.H[1], Dr.N.Sudha[2]
[1]Dept of Computer Science and Engineering
[2]Professor, Dept of Computer Science and Engineering
[1, 2] CMS College of Engineering and Technology,Coimbatore,Tamil Nadu,India

Abstract- *Wireless Sensor Networks (WSNs) presume that sensor nodes spontaneous cooperate in order to work correctly. This collaboration process is based on performance and quality.And then some nodes can rubbish to this performance, finding to effecientnode processing. Thus, the whole network process could be affected. The use of previousframeworkis well to find effectivenodes. However in this process more energy used for detecting process and lack of network lifetime, to overcome this above problem, we propose a new method based on a secret parameterallocationformajorprecaution in all type of Networks. In Wireless Sensor Networks, the estimation load and complication for key management is mainly subject to limitation of the node's accessible resources and the aggressivepersonality of network. In this proposed work, we present anefficient and secure key management named as Random Key Pre-distribution for wireless sensor networks (WSN) that builds keys by applying a classifieddisseminationtechnique and an elemental multicast cluster group. We propose a key pre-distribution scheme that relies on probabilistic key sharing among nodes within the sensor network. Key pre-distribution is the method of distribution of keys onto nodes before deployment*

Keywords- Wireless Sensor Networks, Clustering, efficient and secure key management, multicast routing, data sharing.

I. INTRODUCTION

A wireless sensor network (WSN) is a network designed by a huge amount of sensor nodes, each armed with sensor(s) to detetminenatural phenomena such as temperature , light, motion, or sound. The wireless sensor network (WSN) is manufactured by a "nodes" from a sporadic to some hundreds or equal thousands, wherever each node is attached to one sensor. A wireless sensor network (WSN) node is also known as mote, it is commonly providing with one or number of sensors to get data about the near bycoverage area. The different sensors to use, wireless sensor network(WSN) can be executed to support many applications composed with security, entertainment, military sensing and tracking, patient status monitoring, process automation, industrial monitoring, traffic flow monitoring, public utilities, and asset management.

Though, many wireless sensor network (WSN) devices have simple source constraints in terms of energy, threshold, calculation, and memory, produced by a requirement to limit the cost of the large number of devices essential for various applications and by settings that avoid easy admittance to the devices. In order to in previous process dynamically give each node validation and establish a pair wise key between nodes, we usedkey management by using a un pairedcertificate less hybrid signcryption theme (CL-HSC) planned by America in AN earlier work [10], [11]. CL-EKM is scalable just in case of additives of new nodes once network preparation. CL-EKM is secure against node compromise, biological research and impersonation, and ensures forward and backward secrecy.
For overcome this limitations we move on new technique.In this paper, we presentaefficient and secure key management framework for Wireless Sensor Networks. In our proposed we using RKP (Random Key Pre-distribution) RKP schemes have several variants.

Their system works by distributing a key ring to each participating node in the sensor network before deployment. Key pre-distribution is the method of distribution of keys onto nodes before deployment. Secret keys are generated, placed in sensor nodes and each sensor node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph.

We useNetwork Simulator as a simulator to perform the current method. part II explain the background information about the key management schemes. part III discuss about the new proposed method. Finally simulation and results are discussed in part IV.

II. RELATED WORK

According to the secure communication demand in wireless sensor network (WSN),varieties of key foundations are needed. One is pair wise key foundation; the opposite is cluster key foundation. A few schemes has been projected that incorporates 3phase normally [10]:(1) key setup before deployment, (2) shared-key discovery once construction, and (3) path-key foundation if 2 sensor nodes don't share an on the spot key. The most in style pair wise key pre-distribution answer is Random Pair wise Key theme [11] which addresses unessential storage drawback and provides some key flexibility. It's supported Erodes and Reni's [9] work.
Every sensing element node stores a random set of Nape pair-wise keys to target chance p that 2 nodes are connected. Neighbouring nodes will tell if they share a common pair-wise key once they send and receive-"Key Discovering" Message inside radio range. Its defect is that it sacrifices key property to contract the storage usage. Closest (location-based) pair-wise keys pre-distribution theme [8].

It takes benefit of the situation data to enhance the key connectivity. Later on, Random key-chain based most of the key pre-distribution result is another random key pre-distribution solution that originated from the answer of basic probabilistic of keyreconstract scheme [9]. It depends on probabilistic.There are many key reinforcement greetings to build up security of the established link keys, and improve resilience. Objective is to firmly generate a fresh link or path key by using established keys, so the secret's not com- secure once one or a lot of sensing element node is recorded. One method is to extend quantity of key overlap needed in shared key discovery phase.

Q-composite randomly generated key pre distribution theme [11] needs letter common keys to establish a link key. Similar mechanism is projected by Pair-wise key foundation protocol [6] that uses threshold secret sharing for key reinforcement. Chuang et al. [7] and Agawam et al. [8] scheduled a two-layered key management theme and a dynamic key update protocol in dynamic Wireless Sensor Networks (WSN) supported the DaffierHellman (DH), severally. However, both schemes don't seem to be fitted to sensors with limited resources and area unit unable to perform valuable computations with massive key sizes (e.g. a minimum of 1024 bit). Since computer code is estimated additional economical and features a short key length (e.g. 160 bit), many approaches with certificate are planned supported computer code. However, since every node should exchange the certificate to determine the pair wise key and verify every other's certificate previously use, the communication and computation overhead increase dramatically.

Also, the Base Station (BS) suffers from the upward of certificate management. Furthermore, existing schemes don't seem to be secure. [5] [3].Huang et al. [4] planned a ECC-based key foundation strategy for self-organizing wireless sensor network (WSN). However, we used to give more protection of their theme. Sattam et al. proposed a Certificate less public key cryptography (CL-PKC), this typicaly used to public key cryptography which escapes the essential escrow of identity based cryptography [8]. Hsun Chuang et al. Cooperate with dynamic pair-wise key and cluster key process are shared in more rounds for key material transaction without encryption/decryption.

Exponentiation processes in Two-layered Dynamic Key Management (TDKM). Sensor nodes (SN) are provided with some degree of properties including energy efficiency, saving capacity, and delay. In academic analysis, Two-layered Dynamic Key Management (TDKM) is correlated with existing key management near display its efficiency.

III. PROPOSED METHOD

We proposed an efficient and secure key management scheme for detecting selfish nodes that combines local ombudsman detections and the dissemination of this information on the network.In this paper, we present a efficient and secure key management framework for Wireless Sensor Networks. In our proposed we using RKP (Random Key Pre-distribution) RKP schemes have several variants.

Their system works by distributing a key ring to each participating node in the sensor network before deployment. Key pre-distribution is the method of distribution of keys onto nodes before deployment. Secret keys are generated, placed in sensor nodes and each sensor node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph.

The intial technique is that headmember form the underlying service group for efficient communication.Forefficient, only a pre member of the cluster nodes initiates theshare update phase in eachround. A ticket based scheme isintroduced for efficient certificate less key less updating. Normally, becauseof share updating, recently joining servers could be idle to the system if they mention outdated unauthorized less key less.

Our schemedoes not isolate new servers, and is open for regular nodes foreasy joining and departing. efficient and secure key management schemecreates a view of certification less authority(CA)andprovides secure and efficient service in the mobile and ad hoc environment. In this framework we achieved high performance and accuracy results.

A. Initialization

In this module used to initialize the nodes in network topology. We used network topology and topography for our network animator window (nam window). We have syntax for create nodes in network animator window. Then we can create nodes in two types like random and fixed motions.

In random motion we fixed range for X and Y, fixed particular range then the nodes are randomly generate in that range of nam window. In fixed motion we give X and Y dimension position for all nodes then all the nodes are fixed in that particular dimension.

Sensor nodes are aware of their own positions. The position information may be based on a global or a local geographic coordinate system defined according to the deployment area. Determining the position of the nodes might be achieved using a satellite based positioning system such as global positioning system (GPS) or one of the energy-efficient localization methods proposed specifically for WSNs.

1) Creation of Structure Parameters: The Key Generation Centre (KGC) at the Base Station (BS) runs the following steps by taking a security parameter k ∈X+ as the input, and returns a list of structure parameter.
$\tau = \{Fi, E/Fi, G, P, Ppub= xP, h0, h1, h2, h3\}$
2) Node Registration: The Base Station (BS) allocates a unique identifier, denoted byCa, to each sensor node nCa and a unique identifier, denoted byCHb, to each cluster head$nCHb$,

where $1 \leq a \leq N1$, $1 \leq b \leq N2$, $N = N1+ N2$.

B. Group formation

Once the nodes are used, all group head through datashares to sensor node. group head to control a group with the approved node and they exchange a normalgroup key. The cluster head also establishes a pairwise key with each member of the cluster. We also assume that the cluster head is$nCHb$with $nCa1 \leq a \leq n$ as clustermembers$nCHb$. Establishes a cluster key forOPb secure communication in the cluster.

The server group structure should be maintained in the entire lifetime of the network.However, for a mesh structure, there are possible multiple paths between pair of servers. Thus if one link is broken the alternative link could be utilized instead of launching the costly procedure for breakage recovery.In RKP, the periodical message Request and Reply are sent out in order to refresh the server group.

i. Distance calculation

The distance between any two fireflies i and j at xi and xj respectively, the Cartesian distance is determined by equation where xi, k is the k th component of the spatial coordinate xi of the i th firefly and d is the number of dimensions.

$$d_{i,j} = \text{Distance}(\mathbf{x}^i, \mathbf{x}^j) = \sqrt{\sum_{k=1}^{n} (x_k^i - x_k^j)^2}$$

ii. Attractiveness

In the Firefly algorithm, there are two important issues: the variation of the light intensity and the formulation of the attractiveness. We know, the light intensity varies according to the inverse square law.

Suppose it is absolute darkness.

Light intensity of each firefly is proportional to quality of solution.

Each firefly needs to move towards the brighter fireflies.

Light intensity reduction abides the law:

$$(I\_0, d)=I\_0/d\text{^}2$$

I_0 is the light intensity at zero distanced
d is the observer's distance from source
If we take absorbtion coefficient "ɣ" into account:

Attractiveness (I_0, d, "ɣ") = I_0 e^(−"ɣ" d^2)
$Ir = Isr$ 2 (1)

Where I(r) is the light intensity at a distance r and Isis the intensity at the source.

When the medium is given the light intensity can be determined as follows:

$$Ir = I0e -\gamma r(2)$$

To avoid the singularity at r=0 in (1), the equations can be approximated in the following Gaussian form:

$$Ir = I0e\ -\gamma r\ 2 \quad (3)$$

As we know, that a firefly's attractiveness is proportional to the light intensity seen by adjacent fireflies and thus the attractiveness β of a firefly is determined by equation (4) where β0 is the attractiveness

$$\text{atr=0.}\ \beta = \beta 0e–\gamma rm(\text{m}\geq 1) \quad (4)$$

iii. Movement

The movement of a firefly i is attracted to another more attractive (brighter) firefly j is determined by

$$xi = xi + \beta 0e\ -\gamma rij\ 2\ xj - xi + \alpha E$$

Movement consist two elements

- Approach to better solutions
- Move randomly

C. Key Generation & Authentication

In this module, security is based on the multiplicative group. The corresponding private pairing parameters are preloaded in the sensor nodes during the protocol initialization. In this Module, the key cryptographies used in the protocol to achieve secure data transmission, which consist of symmetric and asymmetric key based security. This scheme enables the intermediate nodes to authenticate the message so that all corrupted message can be detected and dropped to conserve the sensor power. It proposed an efficient key management framework to ensure isolation of the compromised nodes.

Key management deals with the secure generation, distribution, and storage of keys. It plays a vital role in computer security today as practical attacks on public-key systems are typically aimed at key management as opposed to the cryptographic algorithms themselves. This report will investigate the techniques used in the distribution of secret keys used to decrypt and encrypt messages with particular focus key distribution scheme.

Types of Keys

• **Certificateless Public/Private Key**: Before a node is deployed, the KGC at the BS generates a unique certificateless private/public key pair and installs the keys in the node. This key pair is used to generate a mutually authenticated pairwise key.

• **Individual Node Key**: Each node shares a uniqueindividual key with BS. For example, a L-sensor can usethe individual key to encrypt an alert message sent tothe BS, or if it fails to communicate with the H-sensor.AnH-sensor can use its individual key to encrypt themessage corresponding to changes in the cluster. The BS can also use this key to encrypt any sensitive data, such as compromised node information or commands. Before a node is deployed, the BS assigns the node the individual key.

• **Pairwise Key**:Each node shares a different pairwise keywith each of its neighboring nodes for secure communications and authentication of these nodes. For example, in order to join a cluster, aL-sensor should share a pairwise key with theH-sensor. Then, the H-sensor can securely encrypt and distribute its cluster key to the L-sensor by using the pairwise key. In an aggregation supportive WSN, theL-sensor can use its pairwise key to securely transmit the sensed data to the H-sensor. Each node can dynamically establish the pairwise key between itself and another node using their respective certificateless public/private key pairs.

• **Cluster Key**:All nodes in a cluster share a key, named ascluster key. The cluster key is mainly used for securing broadcast messages in a cluster, e.g., sensitive commandsor the change of member status in a cluster. Only the cluster head can update the cluster key when aL-sensor leaves or joins the cluster.

Now in this section we deliver the pairwise key update and cluster key update processes.

1) Pairwise Key Update: Only sensor nodes can update their pairwise key. Toward update a pairwise encryption key, two nodes are to sharedthe pairwise key perform for in a Pairwise Encryption Key Establishment process.

2) Cluster Key Update: Only cluster head can update their cluster key. If a sensor node attempts to change the cluster key, the node is considered a malicious node.

The scheme also includes three phases:

(1) key predistribution,
(2) shared key discovery
(3) path key establishment.

3.3.1 key pre-distribution

Before the deployment of nodes, for each node, a control center (CC) randomly chooses a key ring and loads it into the node. RKP schemes have several variants. Here proposes a key pre-distribution scheme that relies on probabilistic key sharing among nodes within the sensor network. Their system works by distributing a key ring to each participating node in the sensor network before deployment.

This key agreement problem is a part of the key management problem, which has been widely studied in general network environments. There are three types of general key agreement schemes: trusted-server scheme, self-enforcing scheme, and key pre-distribution scheme. The trusted-server scheme depends on a trusted server for key agreement between nodes. This type of scheme is not suitable for sensor networks because there is usually no trusted infrastructure in sensor networks. The self-enforcing scheme depends on asymmetric cryptography, such as key agreement using public key certificates. Any pair of nodes can use this global master secret key to achieve key agreement and obtain a new pair-wise key. This scheme does not exhibit desirable network resilience: if one node is compromised, the security of the entire sensor network will be compromised.

3.3.2 shared key discovery

The shared-key discovery phase takes place during DSN initialization in the operational environment where every node discovers its neighbors in wireless communication range with which it shares keys. The simplest way for any two nodes to discover if they share a key is that each node broadcast, it has in mind, the list of identifiers of the keys on their key ring. This approach does not give an adversary any attack opportunity that he does not already have. For example, if an adversary captures a node he can discover which key of that node is used for which link by decrypting communications; and if he does not capture a node, the adversary can mount a traffic analysis attack in the absence of key identifiers.

3.3.3 Path key establishment

The path-key establishment phase assigns a path key to select pairs of sensor nodes in the wireless communication range that do not have a common key, but are connected by two or more links at the end of the shared-key discovery stage. Path keys need not be generated by sensor nodes. The design of the DSN ensures that, after the shared-key discovery phase is finished, a number of keys on a key ring are left unassigned to any link. For instance, both analysis and simulations indicate that even without special provisioning a substantial bit of keys are left unused on key rings. Provisioning for sufficient ring keys that are left unassigned by the determination of key-ring size (k) can also anticipate both the effects of revocation and those of incremental gain of new sensor nodes, since both may require the carrying out of the path key establishment phase after shared-key discovery.

IV. RESULTS AND DISCUSSION

We use Network simulator version-2 (NS2) to show the performance of our proposed scheme. A wireless sensor network (WSN) consists of30 sensornodes are randomly deployed over a square region of 1000 ×1000 m2 used in this simulation. The size of the data packet is 512 bytes. Ad hoc on Demand Routing (AODV) protocol is used. We have cluster groups.

As compared to existing scheme, our proposed scheme has better performance in terms of energy consumption, Lifetime, and throughput. The following section shows the simulation parameters, results and comparison performance of the proposed system.

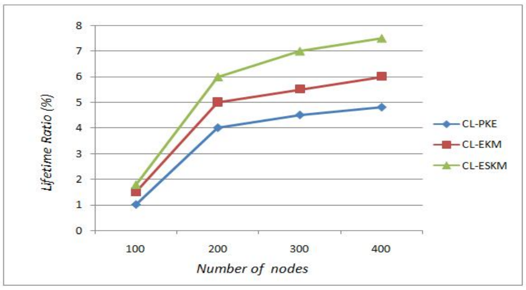
Simulation Parameters

Parameter	Value
Field size	1000×1000 m
Number of sensor nodes	30
Propagation type	Two ray ground
Routing type	AODV
Channel	Wireless channel
Simulation Time	85.0 seconds

Performance Results

In this section, the performance of our protocol is compared with the existing method in terms of Lifetime,and throughput.

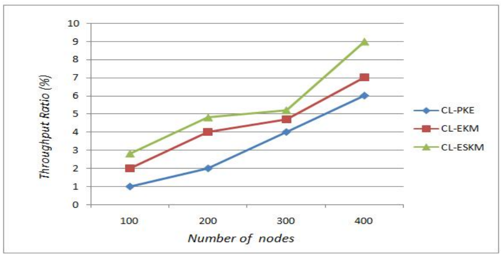
NetworkLifetime



Above graph shows the comparison of existing and proposed key management scheme in terms of Lifetime. In this figure, the performance of proposed key management scheme is increased lifetime ratio level as compared to existing key management scheme.

ThroughputRatio

Bellow graph shows the comparison of existing and proposed key management scheme in terms of Throughput. In this figure, the performance of proposed key management scheme is good Throughput level as compared to existingkey management scheme.



V. CONCLUSION

Due to internet connectivity security is an important issue for ad hoc mobile networks. For security we mainly consider the following attributes: availability, privacy, integrity, authentication, authorization and non-denial. Certain security techniques and methods have been construct and present for wireless Ad-hoc network. Key management is the central aspect of the security of wireless sensor networks, and it is still a pathetic condition. In this paper we propose a new key management scheme, RKP framework,

Based on the secret sharing scheme, where the system secret is sharing to a cluster of head nodes. The headercluster creates a view ofcertification less authority(CA). The advantage is that in RKP it is easier for a node to request service from a well maintained group rather than from multiple "self-governing" service providers which may be spread in a whole area. In Efficient and Secure Key Management the server group provides certificate less key less update service for all nodes including the servers themselves.

REFERENCES

[1] Akyildiz I.F., Su W., Sankarasubramaniam Y., and Cayirci E., "A Survey on Sensor Network", IEEECommunication Magazine, vol. 40, no. 8, Aug. 2002, pp. 102-114.

[2] Alagheband and Aref., "Dynamic and secure key management model for hierarchical heterogeneous sensor networks"

[3] Carman D. W., Krus P. S, and Matt B. J, Constraints and approaches for distributed sensor network security". Technical Report 00-010, NAI Labs, Network Associates, Inc., Glenwood, MD, 2000.

[4] Hsun Chuang I., Wei-Tsung Su, ChunYiWu,Jang-Pong Hsu, Yau-Hwang Kuo.,"Two-layered Dynamic Key Management inMobile and Long-lived Cluster -based Wireless Sensor Networks".,Dept. of Comput. Sci. & Inf. Eng., National Cheng Kung Univ., Tainan.

[5] Huang, Q.; Cukier, J.; Kobayashi, H.; Liu, B.; Zhang, J.," Fast Authenticated Key Establishment Protocols for Self-Organizing Sensor Networks" TR2003-102 February 2004.

[6] Jiang P., "A new method for node fault detection in wireless sensor networks," Sensors, vol. 9, no. 2, pp. 1282–1294, 2009.

[7] Lazos L., and Poovendran R.,. "Serloc: Robust localization for wireless sensor networks".ACM Trans. Sen. Netw., 1(1):73–100, 2005.

[8] Liu, D. and Ning P. 2003. Establishing pairwise keys in distributed sensor networks. In CCS '03: Proceedings of the 10th ACMconference on Computer and communications security. ACM, New York, NY, USA, 52−61.

[9] Liu D., and Ning P., "Efficient distribution of key chain commitments for broadcast authentication in distributed sensor networks". In Proceedings of the 10th Annual Network and Distributed System Security Symposium, pages 263–276, 2004.

[10] ParadisL.and Han Q., "A survey of fault management in wireless sensor networks," J. Netw. Syst. Manage., vol. 15, no. 2, pp. 171 –190, 2007.

[11] Perrig A., Szewczyk R., Tygar J. D., Wen V., and Culler D. E. "Spins: security protocols for sensor networks". Wireless Networking, 8(5):521–534, 2002.