`

Enhancing Three Tier Security Scheme For Wireless Sensor Network

Sumathi. N, Rajesh R. S
Department of Computer Science & Engineering
Manonmaniam Sundaranar University
Tirunelveli-627 012

***Abstract* – Security is a major issue in WSN. This article describes a three-tier general framework that permits the use of pair wise key pre-distribution scheme and Polynomial based key distribution. The new framework requires two separate key pools, one for the mobile sink to access the network, and one for pair wise key establishment between the sensors. Through the Detailed Analysis having the number of sensor nodes with Sink. Sinks are Static and Dynamic. Experiments taking number of sensor nodes with Attacker and without Attacker. Analyses the Performance using Probability and Hash value. To further reduce the damages caused by stationary access node replication attacks, we have strengthened the authentication mechanism between the sensor node and the stationary access node in the proposed framework.**

Index Terms – Key distribution; pair wise key; symmetric key cryptography, one way hash chain, Message digests.

I. INTRODUCTION

A wireless sensor network (WSN) consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, sound, pressure, etc. and to cooperatively pass their data through the network to a main location The major challenges to be addressed in WSNs are coverage and deployment, scalability, quality-of-service, size, computational power, energy efficiency and security. Among these challenges, security is a major issue in wireless sensor networks. Therefore security services such as authentication and pair wise key establishment between sensor nodes and mobile sinks are important. The problem of authentication and pair wise key establishment in sensor networks with Mobile Sink is still not solved in the face of mobile sink replication attacks .For the basic probabilistic and q-composite key pre-distribution schemes ,an attacker can easily obtain a large number of keys by capturing a small fraction of the network sensor nodes making it possible for the attacker to take the control of the entire network by deploying a replicated mobile sink and then initiate data communication with any sensor node.

One of the major abilities that the sensors have is that they gathered the acts of sensing, data processing, and communicating components together. The positions of the sensors and communications topology are carefully engineeredSensor nodes are small embedded devices which are mainly able to perform simple computations and to send/receive data. Their typicalusage is to gather information about their Environment via sensors. Because of cost and energy constraints, only one node is generally able to transmit data from the sensor network to the "outside world "by means of a longer-range connection. This node is called a sink since it acts as such with regards to the DataStream coming from the network computations are performed and data are fused.

A. Motivation And Justification

The sensor nodes monitor a geographical area and collect sensory information. Access points act as a central transmitter and receiver of sensor network. Key management is used to establish the pair wise keys in WSN networks. These keys are used in encryption and decryption process. In a symmetric key algorithm the keys involved are identical for both encrypting and decrypting a message. An encryption key that is used by everyone on the network or in the vicinity. Contrast with an "individual key" that is used for only one user, also called "pair wise key," "per-station key" and "unique key." key lengths of 128 bits (for symmetric key algorithms).In the proceeding system used the pair wise key and the Symmetric Cryptographic Key.

B. Organization Of The Paper

Rest of the paper is organized as follows. In section.II, related works of the key distribution were done. Section.III key generation and key discovery mechanisms are discussed. And section.IV is the experiments and performance results. Finally, section.IV is the conclusion and the future scope.

II. RELATED WORK

Y. Tirta et.al. [1]. Proposes "Efficient collection of Sensor Data in Remote Fields Using Mobile Collectors,'' describes a single collector and analyze three schedules for the collector to visits the cluster heads. The schedules are (a) Round-Robin schedule: the collector visits each cluster head to collect data in a round-robin manner. (b) Data-Rate Based schedule: the frequency of visiting a cluster head is proportional to the aggregate data rate from all the nodes in the cluster. (c) The Min Movement schedule: the collector visits the cluster heads in the proportion of the aggregate data rate, but also with the goal of reducing the distance traversed. It is used to collect sensor's data from remote field's using

mobile collectors. Low latency and Energy Minimization is the Advantage. The Disadvantage in this system is did not detect the node failure. It is not used in large scale sensor networks.

L.Eschenauer et.al. [2]. proposes "A Key-Management Scheme for Distributed Sensor Networks,'' describes the Distributed sensor network using an Ad-hoc network. Node Arrangement using a Random graph method. Protocol used to protect data. Create a shared-key discovery and path-key establishment. Symmetric key pre-distribution scheme used. Nodes are grouped. Because of group communication accommodated. Here occurred a collision, high cost, and high processing time. Encryption methods and hash functions for protecting DSN Additional node adding, key-revocation and re-keying are possible. Data Encrypted using RSA cryptography method.RSA method using only a smaller distance. The advantage is Addition and Deletion of sensor node as possible. The disadvantage is RSA processing will be high.RSA not provide the full security and time will be increased.

D. Liu et.al. [3]. Proposes Establishing, "Pair wise keys in Distributed Sensor Networks,'' describes, Using Pair-wise keys in Distributed Environment, Using KDC and also used the public key cryptography. Polynomial-based key distribution protocol used to set the keys. Using two mechanisms to set the keys. Pair wise key establishment is a fundamental security service in sensor networks; to facilitate the study of novel pair wise key pre distribution techniques, it presents a general framework for establishing pair wise keys between sensors on the basis of a polynomial-based key pre distribution protocol. For security using µTESLA method .The advantage of this indicates that these two schemes have a number of properties, including high probability (or guarantee) to establish pair wise keys, tolerance of node captures, and low communication overhead. It presents a technique to reduce the computation at sensors required by these schemes. The disadvantage is Computational overhead is high, so affect DOS Attack, so not secured.

H.Chan et.al. [4]. Proposes. "Key Distribution Techniques for Sensor Networks'', describes two techniques 1.Key Distribution, 2. Key Establishment. Key Distribution Scheme using Random Key Pre distribution. In this Random key pre distribution used Asymmetric Key Cryptography. All keys are shared in Pair-wise method. q-composite Prekey distribution method used in random key scheme. The advantage is improving the Network Security. The disadvantage is need large number of keys, because using the keys are Single-space Pair wise key and Multi-space Pair wise key. Storage space low, so affect DDOS (Distributed Denial of Service).

C.Blundo et.al. [5]. Proposes "Perfectly-Secure Key Distribution for Dynamic Conferences'', describes Key Distribution Scheme is used to distribute Private individual keys to a set of users in an off-line trusted servers. Using Non-iterative Model to compute the common key without any iteration. Non-iterative model to provide a common key's for individual identities. The method associated for Hyper Graph Communication Structure. Authentication of conference members based on cryptosystems without the need of on-line server. The key distribution is related to the session key functions. The advantage is a Network Topology is not a complete graph. The disadvantage is using number of keys, does not convey any information to another keys.

III KEY GENERATION AND KEY DISCOVERY MECHANISM

A. Three-Tier General Framework

In the new security framework [6] a small fraction of the preselected sensor nodes called the stationary access nodes; act as authentication access points to the network. It triggers the sensor nodes to transmit their aggregated data to mobile sinks. A mobile sink sends data request messages to the sensor nodes via a stationary access node. These data request messages from the mobile sink will initiate the stationary access node to trigger sensor nodes, which transmit their data to the requested mobile sink.

B. Pair-Wise Key Establishment Scheme

In this scheme use two separate polynomial pools: the mobile polynomial pool and the static polynomial pool. Use the mobile polynomial pool [12] to connect mobile nodes with the stationary nodes of the network. The static polynomial pool is used to securely connect stationary nodes of the network.

C. Polynomial -Pool- Based Key Predistribution

Polynomial-pool-based key pre distribution scheme is based on the idea presented by Blundo et al. Let p be a finite field with q just large enough to accommodate a symmetric encryption key. Fig 1 provides the key distribution process for a 128-bit block cipher. Two shares f (α) and f (β) of the same polynomial f satisfy

f (α) (ß) = f (ß, α) = f (α, ß) = f(β) (α) . α

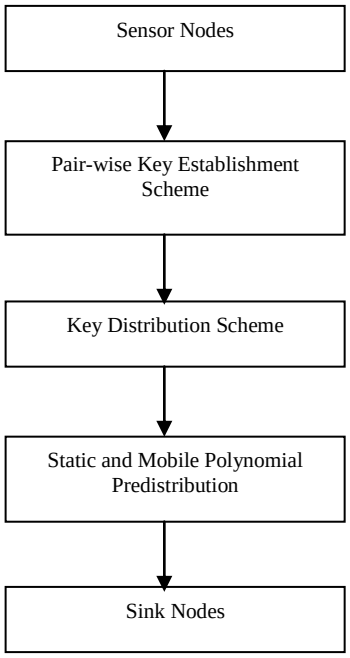


Fig.1. key distribution Process

D. Key Discovery Mechanism

- Key: symmetric key which is used to secure communication among two or more sensor nodes
- Keying materials: any kind of information and algorithms which are used to generate keys
- Credentials: keys, keying materials and algorithms
- Key-chain: list of keys or keying materials which are stored on a sensor node
- Key-pool: list of all keys or keying materials which are used in the WSN
- Path-key: key which is used to secure communication over multi-hop wireless links through one or more sensor nodes
- Pair-wise key: key which is used to secure unicast communication between a pair of sensor nodes over single or multi-hop wireless link

1. *Static and Mobile Polynomial Pre Distribution*

This is performed before the nodes are deployed. A mobile polynomial pool M of size |M| and a static polynomial pool S of size |S| are generated along with the polynomial identifiers. All mobile sinks and stationary access nodes are randomly given Km and one polynomial (Km >1) from M. The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every stationary access node .This assures that [11] a mobile node shares a common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured. All sensor nodes and the preselected stationary access nodes randomly pick a subset of Ks and Ks-1 polynomials from S.

2. *Key Discovery between Mobile Node and Stationary Node, Sensor Node and Stationary Node*

In order to establish a pair wise key [9] between sensor node u and mobile sink v, a sensor node u needs to find a stationary access node a in its neighborhood in both mobile sink v and sensor node u. Stationary access node needs to establish pair wise keys with both mobile sink v and the sensor node .It has to find a common mobile polynomial with the mobile sink and a common static polynomial with the sensor node .To discover a common mobile/static polynomial a sensor node I may broadcast a list of polynomial IDs. We provide an encryption list α, where Kv is a potential pair wise key and the other node may have as suggested. When a direct secure path is established between nodes u and v, mobile sink v sends the pair wise key Kc to node a in a message encrypted and authenticated with the shared pair wise key Kv,a between v and a if node a receives the above message and it shares a pair wise key with u, it sends the pair wise key Kc to node u in a message encrypted and authenticated with pair wise key Ka,u between a and u [10]. If there is any fail in the direct key establishment, the mobile sink and the sensor node will have to establish a pair wise key with the help of other sensor nodes.

To establish a pair wise key with mobile sink v, a sensor node u has to find a stationary access node a in its neighborhood such that node a can establish a pair wise key with both nodes u and v. If node a establishes a pair wise key with only node v, sensor node u needs to find an intermediate sensor node i along the path u-i-a-v.

- U and V are the communicating nodes.
- IDU is the ID of a node U
- KU, V is the secret key between nodes U and V used for communication between these two nodes.
- N is the total number of nodes deployed initially
- M is the average number of neighbors that a typical sensor node has.
- R is the transmission range of a node
- ENCKU, V (M)) is the message M encrypted with key shared between the nodes U and V.

E. Key Generation:

Key generation [8] is the process of generating keys for cryptography. Figs 2 provide the key generation and Authentication process. A key is used to encrypt and decrypt whatever data is being encrypted/decrypted. The pair wise key will generate from shared polynomial:

Step 1: Node u evaluates gu(y) at y = v, and represents the evaluation result in l binary bits.

Step 2: It uses the most significant l − r bits of gu (y), denoted as Ku, v, as the key.

Step 3: Node u sends h (Ku, v) to node v

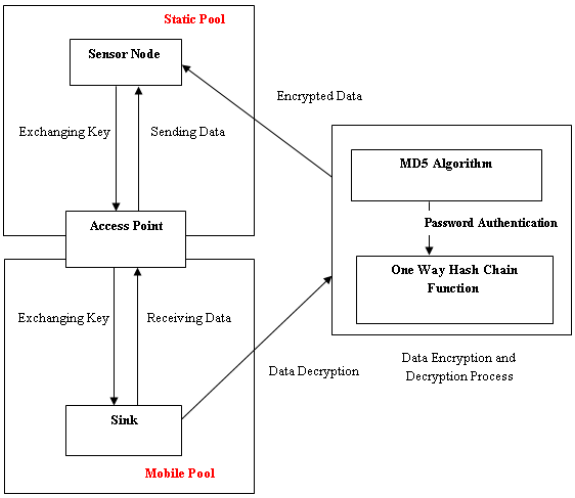


Fig.2 Key Generation and Password Authentication

❖ *Key ring and key pool Size:*

Due to the limited communication capabilities a number of nodes with which a particular node can communicate is n'<<n. This means that the probability of two nodes sharing at least one key in their key rings of size k is p'=d/(n'-1)>>p Key pool size P can be derived as a function of k:

$$p = 1 - \frac{(1-\frac{k}{p})2(p-k+1/2)}{(1-\frac{2}{p}k)(p-2k+1/2)}$$

1. Polynomial Key Distribution Scheme

Polynomial based key pre-distribution scheme reduces the amount of pre-distributed information still allowing each pair of nodes to compute a shared key. Polynomial based key distribution scheme provide large amount of key storage place.

- *Polynomial based key pre-distribution: initialization*

❖Special case: λ=1
❖Each node has an id r_U which is unique and is a member of finite field Z_p
❖Three elements a, b, c are chosen from Z_p
❖Polynomial f(x,y) = (a + b(x + y) + cxy) mod p is generated
❖For each node polynomial share $g_u(x) = (a_n + b_n x)$ mod p

Where, $a_n = (a + br_U)$ mod p and $b_n = (b + cr_U)$ mod p is formed and pre-distributed

- *Polynomial based key pre-distribution: key discovery*

In order for node U to be able to communicate with node V the following computations have to be performed:

❖$K_{u,v} = K_{v,u} = f(r_u, r_v) = (a + b(r_u + r_v) + cr_u r_v)$ mod p
❖U computes $K_{u,v} = g_u(r_v)$
❖V computes $K_{v,u} = g_v(r_u)$

2. Static and Mobile Polynomial Pre-distribution:

This is performed before the nodes are deployed. A mobile polynomial pool and a static polynomial pool are generated along with the polynomial identifiers. All mobile sinks and stationary access nodes are randomly given. One polynomial from Mobile polynomial pool. The number of mobile polynomials in every mobile sink is more than the number of mobile polynomials in every stationary access node. This assures [7] that a mobile node shares a common mobile polynomial with a stationary access node with high probability and reduces the number of compromised mobile polynomials when the stationary access nodes are captured. All sensor nodes and the preselected stationary access nodes randomly pick a subset of key from static pool. They are analyzed the performance of the proposed scheme using two metrics: security and connectivity. For security, present the probability of a mobile polynomial being compromised; hence, an attacker can make use of the captured mobile polynomial to launch a mobile sink replication attack against the sensor network.

F. MD5 Message Digest Algorithm

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of security applications. It is also commonly used to check data integrity. One-way function: d=h (m) but no h' (d) =m. cannot find the message given a digest. Cannot find m1, m2, where d1=d2.Arbitrary-length message to fixed-length digest.

Bits need for Function:

- m bits data, takes $2^{m/2}$ to find two with the same hash
- 64 bits, takes 2^{32} messages to search (double)
- Need at least 128 bits
- Encryption: challenge r_A, $MD(K_{AB}|r_A)$
- Decryption: r_B, $MD(K_{AB}|r_B)$

G. One-Way Hash Function

One-way hash function is designed in such a way that it is hard to reverse the process, that is, to find a string that hashes to a given value (hence the name one-way.) A good hash function also makes it hard to find two strings that would produce the same hash value. All modern hash algorithms produce hash values of 128 bits and higher. A one-way hash function, also known as a message digest, fingerprint or compression function, is a mathematical function which takes a variable-length input string and converts it into a fixed-length binary sequence. All modern hash algorithms produce hash values of 128 bits and higher. Even a slight change in an input string should cause the hash value to change drastically. Even if 1 bit is flipped in the input string, at least half of the bits in the hash value will flip as a result. This is called an avalanche effect. Since it is computationally infeasible to produce a document that would hash to a given value or find two documents that hash to the

same value, a document's hash can serve as a cryptographic equivalent of the document. This makes a one-way hash function a central notion in public-key cryptography. We provide a digital signature for a document, no longer need to encrypt the entire document with a sender's private key. It is sufficient to encrypt the document's hash value instead. Although a one-way hash function is used mostly for generating digital signatures, it can have other practical applications as well, such as secure password storage, file identification and Message Authentication Code (MAC.)

IV. EXPERIMENTS AND PERFORMANCE EVALUATION

A typical threat known as node replication attack or clone node attack, where an adversary creates its own low-cost sensor nodes called clone nodes and misinforms the network to acknowledge them as legitimate nodes. To instigate this attack, an adversary only needs to physically capture one node, and after collecting all secret credentials (ID, cryptographic keys, etc.), an adversary replicates the sensor node and deploys one or more clones of the compromised node into the network at strategic positions, damaging the whole network by carrying out many internal attacks. we provide a security and detection schemes against to detect the node replication attack.

1. Replication Attack:

Wireless Sensor Networks (WSphysically capture some of the nodes. Once a node is captured, adversary collects all the data) is often deployed in hostile environments as static or mobile, where an adversary can credentials like keys and identity etc. The attacker can re-program it and replicate the node in order to eavesdrop the transmitted messages or compromise the functionality of the network. In particularly a harmful attack against sensor networks where one or more node(s) illegitimately claims an identity as replicas is known as the node replication attack. The replication attack can be exceedingly injurious to many important functions of the sensor network such as routing, resource allocation, misbehavior detection, etc.

2. Analyses The Security Performance:

To analyze the security performance of the Enhanced three-tier scheme, first estimated probability of a Non compromised sensor node being under a stationary access node replication attack, when x number of nodes was being captured. Then estimate the probability of compromised nodes being under the replication attack. Then, find the hash value of the both.

1. without Attacker:

To analyze the security performance of the enhanced three-tier scheme, first estimated probability of a non compromised sensor node being under a stationary access node replication attack, when number of nodes were being captured. First analyze the result under the probability of an algorithm without attacker. Here they got the two polynomial key pool where the mobile pool and the static pool. If a communication is processed between the sensor nodes and the access nodes then they getting the key form the static polynomial pool. If the connection between the mobile sink and access nodes then they getting the key from the mobile pool. The sensor node sending data to mobile nodes put the access point in between the transmission. Experiments analyses the performance using number of sensor nodes at 25, 50, 75, and 100.

25 nodes – 1 sink (Moving & Static)
50 nodes – 2 Sinks (Moving & Static)
75 nodes – 3 Sinks (Moving & Static)
100 nodes – 4 Sinks (Moving & Static)

- *Probability Estimation Function:*

The probability is calculated using the sending and receiving data capacity. During the transformation is processed by the access nodes got the data loss under the circumstances of data hacking. Here the methodology doesn't implement any attacker part. Table 1 analyses the security performance at the number of nodes at 25. Take number of experiments based on the attacker nodes included in the network.

Probability= (recv packet/send packet)*100
In that graph X axis= No of Attacker Nodes
Y axis = Probability
Table 1: Probability Estimation without Attacker

No of Nodes in Process	No of Sink nodes in Process	Probability Estimation
25	1	0.12
50	2	0.11
75	3	0.10
100	4	0.11

- *Hash value:*

Then the data transfer function is processed by the exchanging key under the key pools. Nodes are exchanging key between them by getting the key from pools. The pools allocated the keys using the hash values. So here we also calculated the key values for the hash. Finding the process time by starting time and ending time.

Process Duration = Starting time – Ending time

Table 2 calculate the hash value by the number of packets of data has to send form the sensors and receiving from the receivers. Here they use the highest hash packet value to estimate the hash value. The resulting value to be plot the graph.

Hash Value= hashPkts/ (highest_packet_id+1))*100
In that graph X axis= No of Attacker Nodes
Y axis = Hash value
Table 2: Hash Value Estimation without Attacker

2. with Attacker:

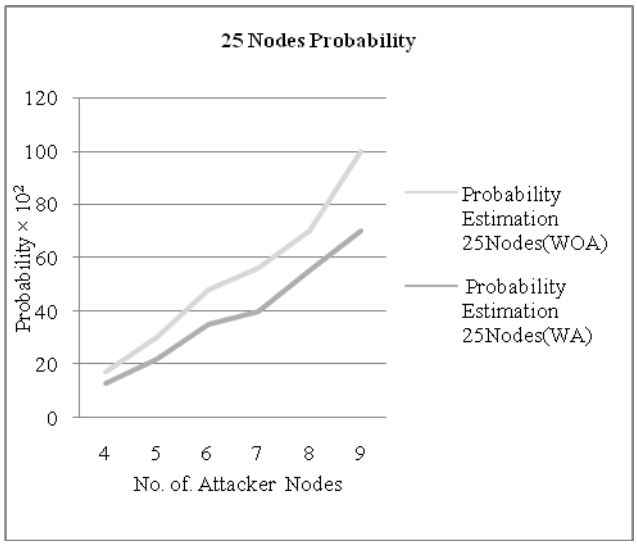
This is analyzing the result under the probability of our algorithm with attacker. Here some nodes are indicated as an attacker. Our methodology is to find the replication attacker nodes and preventing the data which to be sending. Detecting the attacker probability and the data transferring probability has to estimate under these circumstances. Here the attacker is hacking the data from the sensor nodes and then it lost. So they are getting the data loss. Hash key value is also increased to protect the data. Attacker only compromised the sensor nodes, but don't open the message content. The message contents are protect to using the cryptographic functions Encryption/Decryption. This experiments take the number of nodes are 25, 50, 75,100. Increase the number nodes and calculate the above probability and Hash values. Table 3 and Table 4 provide probability and Hash value estimation with 25 nodes only. Above experiments shows the graphical results in Fig 3 and Fig 4.

Table 3: Probability Estimated in 25 Nodes

No of Nodes in Process	Attacker Included	Algorithm Detected	Probability	Percentage of attacker detection
25	4	4	0.48	100
25	8	8	0.17	100
25	11	11	0.56	100
25	16	14	0.70	87.5

Table 4: Hash Value Estimated in 25 Nodes

No of Nodes in Process	Attacker Included	Algorithm Detected	Hash Value	Percentage of attacker detection
25	4	4	0.01	100
25	8	8	0.06	100
25	10	10	0.14	100
25	12	11	0.32	91.6
25	16	13	0.46	95.0



No of Nodes in Process	No of Sink nodes in Process	Hash Value
25	1	0.23
50	2	0.25
75	3	0.24
100	4	0.25

Fig: 3. Performance Analysis based on Probability

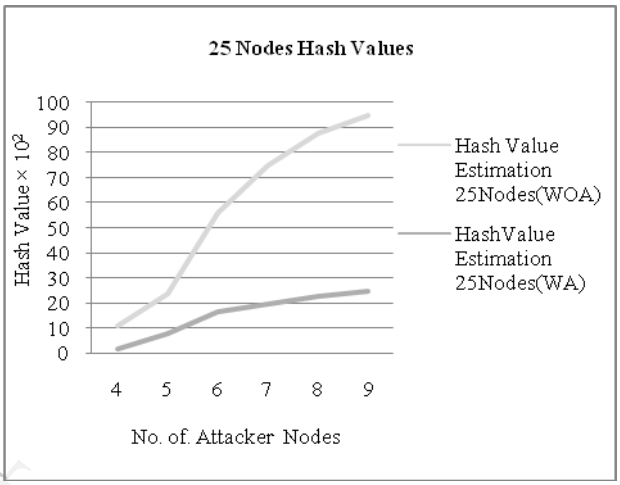


Fig: 4. Performance Analysis based on Hash value

Analyze the security performance of the proposed scheme against a mobile sink replication attack. Previous experiments stated that, for an attacker to launch a mobile sink replication attack on the network, the adversary has to compromise at least one polynomial from the mobile polynomial pool. To achieve this, the adversary must capture at least a specific number of stationary access nodes that hold the same mobile polynomial.

V. CONCLUSION AND FUTURE SCOPE

The work is based on pair wise key and polynomial pool-based key Pre distribution scheme substantially improved network resilience. Strengthening the authentication mechanism using MD5 and one-way hash chain algorithm. Our algorithms effectively detect the replication attack. Analyses the performances based on probability and hash value. Compare the network based on with and without attackers. Without attackers in a network, the probability will be high. Attackers included in a network, hash value will be high to increase the security.

In future this approach has been incorporated in the earlier protocol named as an Efficient and Secure Routing Protocol (ESRP) and enhance the security using Elgamal encryption algorithm and analyses the performance based on throughput, time, delay and PacketDeliveryRatio..

`

REFERENCES

[1] Y. Tetra, Z. Li, Y. Lu, and S. Bagchi (2004), "Efficient Collection of Sensor Data in Remote Fields Using Mobile Collectors," Proc.13th Int'l Conf. Computer Comm. and Networks (ICCCN '04).

[2] L.Eschenauer and V.D. Gligor (2002), "A Key-Management Scheme Distributed Sensor Networks," Proc. ACM Conf. Computer Comm. Security (CCS '02), pp. 41-47.

[3] Liu, P. Ning, and R.Li (2003). Establishing, "Pair wise Keys in Distributed Sensor Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 52-6.

[4] H. Chan, A. Perrig, and D. Song (2004), "Key Distribution Techniques for Sensor Networks," Wireless Sensor Networks, pp. 277-303.

[5] Blundo, A. De Santis, A. Herzberg, S. Kutten (1993), U. Vaccaro, and M. Yung, "Perfectly-Secure Key Distribution for Dynamic Conferences," Proc. 12th Ann. Int'l Cryptology Conf. Advances in Cryptology (CRYPTO '92), pp. 471-486.

[6] Lee, J. and Stinson, D. 2004a. A combinatorial approach to key pre-distributed sensor networks.http:// www. Cacr. Math. Uwaterloo. ca/ _dstinson/ pubs.html.

[7] W.Diffie and M.E.Hellman.New directions in cryptography.IEEE Trans. Inform. Theory, IT-22:644–654, November 1976.

[8] H. Deng, W. Li, and D.P. Agrawal (2002), "Routing Security in Wireless Ad Hoc Networks," Proc. IEEE Comm. Magazine, pp. 70-75.

[9] Duncan S. Wong and Agnes H. Chan. Efficient and mutually authenticated key exchange for low power computing devices. In Advances in Cryptology — ASIACRYPT '2001.

[10] Laurent Eschenauer and Virgil D. Gligor. A keymanagement scheme for distributed sensor networks. In Proceedings of the 9th ACM Conference on Computer and Communication Security, pages 41–47, November 2002.

[11] H. Chan, A. Perrig, and D. Song (2003), "Random Key Pre-Distribution Schemes for Sensor Networks," Proc. IEEE Symp. Research insecurity and Privacy.

[12] Lee, J. and Stinson, D. 2004b. Deterministic key pre-distribution schemes for distributed sensor networks. http:// www. cacr. math. uwaterloo. ca/ _dstinson/ pubs.html.