Efficient Mechanism for Secured Node-Node Data Communication using LU Matrix

Aaditya Mudbhatkal, Chandan Raj.B.R.

Abstract—there should be a mechanism for the secure key establishment for node to node secure data transmission because of constant security threats or attacks. The Adversary can physically capture and get the information contained in the sensor node, eavesdrop and inject new messages, modify the message. The proposed system presents a novel technique for key establishment scheme that is based on LU matrix in which a matrix-based key pre-distribution algorithm is used to achieve node to node secure data or message transmission. The data or message will be sent encrypted with a key shared by sender and the receiver sensor nodes. The user has to enter the number of sensor nodes, transmission range so that all the sensor nodes are deployed within the transmission range and places an event in the sensor network. The sensor nodes within the sensor range specified by the user will sense the event and generates the message. The routing of the data or message between the sensor nodes to the base station or sink is used by Dijikstra's shortest path algorithm to find the shortest path from the sensor node to sink. The RC6 encryption algorithm helps to secure the data or message which is transmitted between the sensor nodes. The outcome of key pre-distribution technique using LU matrix provides node to node mutual authentication and guarantees to find a common keys between any two sensor nodes in the sensor network.

Index Terms — Decryption, Encryption, Event Processing, LU, Matrix, RC6, Wireless sensors

I INTRODUCTION

Wireless Sensor Networks (WSNs) are widely used in many applications today viz., solutions to many challenging problems for both military and civilian applications, including target tracking, battlefield surveillance, intruder detection and scientific exploration. However, using sensors without providing security has resulted to be dangerous in hostile environments.

In many applications of WSN, like military surveillance, security plays a very important role. It is very important to hide secret information from both active and passive adversaries. An adversary tries to act like an authorized node in order to extract important information from a legitimate node. Even if an adversary cannot get to know the confidential information, it can try to disrupt communication or tamper with the messages, so that the wireless sensor network cannot perform the task, for which it was deployed.

The emergence of wireless sensor nodes has allowed practitioners to foresee networking a large set of nodes scattered over a wide area of interest into a Wireless Sensor Networks (WSNs) for large-scale event monitoring and data collection and filtering. Confidentiality, authenticity, availability, and integrity are typical security goals for WSNs. Security issues is the major issue in the Wireless Sensor Network, There are some of the major security attacks on the Wireless Sensor Networks. Some of the attacks are passive which will disclose the secret information of the sensor network and some are really dangerous, These are active attacks from the adversary or an attacker which cause the real damage to the Wireless Sensor Network and nodes .The development of wireless sensor networks was motivated by military applications such as battlefield surveillance; today such networks are used in many industrial and consumer applications, such as industrial process monitoring and control, machine health monitoring, and so on.

The WSN is built of "nodes" – from a few to several hundreds or even thousands, where each node is connected to one (or sometimes several) sensors. Each such sensor network node has typically several parts: a radio transceiver an internal antenna or connection to an external antenna, a microcontroller, an electronic circuit for interfacing with the sensors and an energy source, usually a battery or an embedded form of energy harvesting. A sensor node might vary in size from that of a shoebox down to the size of a grain of dust, although functioning "motes" of genuine microscopic dimensions have yet to be created.

The cost of sensor nodes is similarly variable, ranging from a few to hundreds of dollars, depending on the complexity of the individual sensor nodes. Size and cost constraints on sensor nodes result in corresponding constraints on resources such as energy, memory, computational speed and communications bandwidth. The

topology of the WSNs can vary from simple star network to an advanced multi-hop wireless mesh network.

The propagation technique between the hops of the network can be routing or flooding. If a centralized architecture is used in a sensor network and the central node fails, then the entire network will collapse, however the reliability of the sensor network can be increased by using distributed control architecture. Distributed control is used in WSNs for sensor nodes are prone to failure, for better collection of data and to provide nodes with backup in case of failure of the central node.

II EXISTING SCHEME

A. Related Works

Eschenauer and Gligor [1] (E-G scheme) proposed a random key pre-distribution scheme based on random graph theory and probability theory. According to this scheme, each sensor node receives a different random subset of keys from a large key pool as the node's key ring before deployment and then stores the key ring in its memory. After sensor nodes have been deployed in the designated area, secure direct communication between two nodes requires that nodes share at least one common key. However, one drawback of E-G scheme is that, since the key rings are randomly picked from the same key pool, more than a pair of nodes may use the same common keys to establish their communications. Therefore, these common keys cannot warrant unique authentication.

Du [2] proposed another random key pre-distribution scheme that combined Blom's scheme with random key pre-distribution method. This scheme substantially improves the resilience of the network by using multi hop neighbors. Moreover, it exhibits some threshold when the number of compromised nodes is smaller than the security threshold and the probability of disclosed communication between non-compromised nodes is close to zero.

Liu [3] developed a general framework for key establishment, which is based on the polynomial-based key pre-distribution protocol in Blundo's scheme and the probabilistic key pre-distribution in E-G scheme. This framework is called polynomial pool-based key pre-distribution, which uses a polynomial pool instead of a key pool in E-G and q-composite schemes. The secrets on each node are generated from a subset of polynomials in the pool. If two nodes have the secrets generated from the same polynomial, nodes can compute a shared key based on the common polynomial.

B. New Contributions

In many applications of Wireless Sensor Network, security is a main constraint. Here, a matrix-based key pre-distribution scheme for Wireless Sensor Network is presented. This secure key establishment technique achieves node to node secure data or message transmission. The data or message is sent encrypted with a key that is shared by sender and the receiver sensor nodes. [4][5][6]

This key pre-distribution algorithm is presented for node to node mutual authentication and guarantees to find a common key between any two sensor nodes in the network. The routing of the data or message between the sensor nodes to the base station or sink is achieved through Djikstra's shortest path algorithm. The RC6 encryption algorithm is used to secure data or message transmission between the sensor nodes. [8][9][10]

RC6 encryption is similar to RC5 encryption algorithm but it has many advantages over the RC5 encryption algorithm. Firstly, it uses integer multiplication, quadratic equation and fixed bit shifting for enhanced security. Secondly, its main design objective is its simplicity.

Finally, it is so powerful that it is not reported to be vulnerable to any practical attacks thus making it one of the strongest methods to achieve secured node-node authentication in the sensor network.

III PROPOSED SCHEME

The proposed scheme is concerned with establishing a basic structural framework for a system. It involves identifying the major components of the system and communications between these components. Here, sink is the central node whereas other sensor nodes are in the adjacent areas of the sink.

To reduce communication costs, some algorithms remove or reduce nodes redundant sensor information and avoid data forwarding which are of no use.The data

gathered is saved in the form of hash code or numerical values. Node to node mutual authentication is achieved and security is provided well in this sensor network.

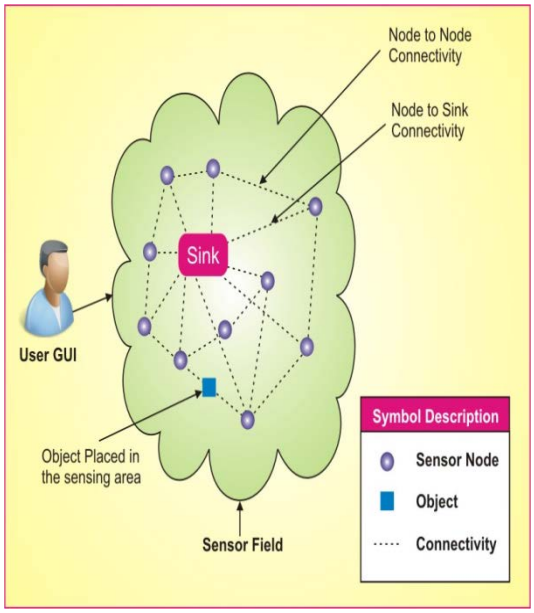

Fig 1. Figure showing a typical sensor node in a sensor network

The sensor nodes are usually scattered in a sensor field as shown in the above figure1. Each of these scattered sensor nodes has the capabilities to collect data and route data back to the sink. Data which are collected are routed back to the sink by a multi-hop architecture through the sink and the collection of sensor node in the sensing area is called the sensor field. The Link level security is provided by using LU Matrix key distribution approach between the sensor nodes.

The Polynomial Pre-distribution Encoding process is decomposed into three processes, 1. Key Establishment Phase, 2. Deployment Phase and 3. Event Processing Phase.

A. Key Establishment Phase

The Key Establishment consists of the following steps. Generating a large polynomial pool each node can pick a subset of polynomials from the large polynomial pool, Form a lower triangular matrix L and upper triangular matrix U, and randomly distribute one row of L and one column of U to each of the sensor node. The random numbers are taken as input to generate the lower triangular matrix and upper triangular matrix. The LU is taken as an input to generate the key matrix which is symmetric.

The key is assigned to each of sensor nodes thus the node-to-node mutual authentication is achieved and rigorously guaranteed to find a common key between any two sensor nodes in the network. Following are the steps for generation of polynomial pre distribution

Step1: Generate a large polynomial pool.

Step2:- Randomly select a group of polynomials from the polynomial pool to form Diagonal elements for the lower and upper triangular matrix

$$\begin{bmatrix} l11 & & \\ & l22 & \\ & & l33 \end{bmatrix} \& \begin{bmatrix} u11 & & \\ & u22 & \\ & & u33 \end{bmatrix}$$

Step3:- Generate the lower triangular matrix elements.

$$\begin{bmatrix} l11 & 0 & 0 \\ l21 & l22 & 0 \\ l31 & l32 & l33 \end{bmatrix}$$

Step4:- By using lower triangular matrix elements and upper triangular diagonal elements will generate upper triangular matrix

$$\begin{bmatrix} u11 & u12 & u13 \\ 0 & u22 & u23 \\ 0 & 0 & u33 \end{bmatrix}$$

Step5:- Node A sends Lri to node B. i.e. selects one row from L matrix

Step6:- Node B obtains Kij by multiplying Ucj (one column from U matrix) with Lri received from node A,

Lri x Ucj = kij.

Step7:- Node B sends Lrj , Kij and its ID S_B to A.

Step8:-Node A obtains Kji by multiplying Uci with Lrj received from B,

Lrj x Uci = kji.

$$\begin{bmatrix} l11 & 0 & 0 \\ l21 & l22 & 0 \\ l31 & l32 & l33 \end{bmatrix} . \begin{bmatrix} u11 & u12 & u13 \\ 0 & u22 & u23 \\ 0 & 0 & u33 \end{bmatrix}$$

$$=$$

$$\begin{bmatrix} k11 & k12 & k13 \\ k21 & k22 & k23 \\ k31 & k32 & k33 \end{bmatrix}$$

K is a symmetric polynomial matrix, thus Kij = Kji .Kji or (kij) is used as the shared polynomial between nodes A and B. Then using the polynomial-based key Pre-distribution node A and node B always find a shared key by evaluating the shared polynomial. The shared key is then found out amongst the sensor nodes in the sensor network. [7]

B. Deployment Phase

The steps involved in the deployment phase include:

1.) Deploy the sink with co-ordinates x and y position.

2.) Deploy nodes, each node having its unique coordinates x and y on the axes.

3.) If any nodes exist within the transmission range of the sink. Then identify such neighbor nodes for the sink

4.) After finding out the neighbor nodes for the sink, draw links between the sink and the node.

5.) Identify the neighboring nodes.

6.) If any node exists within the transmission range of node, then draw the links between corresponding nodes.

7.) Draw sink with x and y parameters.

8.) Draw nodes with parameters x and y

C. Event Processing Phase

This phase consists of three sub phases divided into 3 steps:

1.) Event Process - This process displays the number of nodes sensed in the sensing area.

Step1:-Check whether the nodes are deployed or not. If not, carry on with deployment phase or if deployed, event can be placed in the sensing region.

Step2:-Check if the events are within the sensing range of the sensor nodes. If true, messages are generated and are processed to the sink node. This would give a list of number of nodes sensed in the sensing region.

2.) Event Message Generation – This process generates the packets in the sensor node.

Step 1:- After message is generated, calculate the number of packets to be sent to the nodes or sink.

Step 2:- Decompose the message generated into the number of packets which will be sent to the next process for routing. This would be in the form of message data into packets.

3.) Secure Routing of Messages – This process displays the number of packets which are directly sent into the sink node.

Step 1:- After the packet, generated in the previous process are routed using the neighbor table, check whether the neighbor node id = 0.

Step 2:- If yes, then that sensor node will directly send the packets to the sink or else the packets will be sent to the other neighbor node which has shortest path to sink using Djikstra's shortest path algorithm

IV. SECURITY ALGORITHMS

The processes of encryption and decryption are both composed of three stages: pre-whitening, an inner loop of rounds, and post-whitening. Pre-whitening and post-whitening remove the possibility of the plaintext revealing part of the input to the first round of encryption and the cipher text revealing part of the of the input to the last round of encryption.

1.)RC6 Encryption Algorithm –Following are the steps for the encryption algorithm in which plaintext is stored in four w-bit input registers A, B, C, D, r rounds, w-bit round keys in sequence S[0,…,2r + 3] and the output produced would be the Cipher text produced in A,B,C,D.

*Step*1. First, the registers B and D undergo pre-whitening.

$$B = B + S[0]$$

$$D = D + S[1]$$

*Step*2. There are r rounds, which are designated by the "for" loop

*Step*3. The registers B and D are put through the quadratic equation.

*Step*4. Rotate (log2 w) bits to the left, respectively;

*Step*5. B has an exclusive-or (XOR) operation with A and assigned the value to t;

*Step*6. D has an exclusive-or (XOR) operation with C and assigned the value to u.

$$t = (B \times (2B + 1)) \lll \log_2 w$$

$$u = (D \times (2D + 1)) \lll \log_2 w$$

*Step*7. This value t is then left-rotated u bits and added to round key S[2i],

$$A = ((A \oplus t) \lll u) + S[2i]$$

*Step*8. The resulting value of D and C is left-rotated t bit, added to round key S[2i + 1]

$$C = ((C \oplus u) \lll t) + S[2i+ 1]$$

*Step*9. In the final stage of the round, the register values are permuted, using parallel assignment, to mix the AB computation with the CD computation.

$$(A, B, C, D) = (B,C,D,A)$$

*Step*10. Repeat the *Step* 2 until all the rounds are completed

*Step*11. Finally, registers A and C undergo post-whitening

$$A = A + S[2r + 2]$$

$$C = C + S[2r + 3]$$

2.) RC6 Decryption Algorithm -Following are the steps for the decryption algorithm in which Cipher text stored in four w-bit input registers A,B,C,D and the output generated would be in plaintext stored in A,B,C,D.

*Step*1. Begins with a pre-whitening *Step* for C and A.

$$C = C - S[2r + 3]$$

$$A = A - S[2r + 2]$$

*Step*2. The loop runs in reverse for the number of r rounds

*Step*3. Within the loop, the first task is parallel assignment

$$(A,B,C,D) = (D,A,B,C)$$

*Step*4. Rotated (log2 w) bits to the left, respectively;

*Step*5. From there, the aforementioned quadratic equation is used on D and B.

*Step*6. The resulting value for u, and t respectively, is left-rotated (log2 w) bits

$$u = (D \times (2D + 1)) \lll \log_2 w$$

$$t = (B \times (2B + 1)) \lll \log_2 w$$

*Step*7. The round key S[2i + 1] is subtracted from register C value, the result of which

is right-rotated t bits;

$$C = ((C - S[2i + 1]) \ggg t)$$

*Step*8. Round key S[2i] is subtracted from register A value, the result of which is

Right-rotated u bits.

$$A = ((A - S[2i]) \ggg u)$$

*Step*9. This resulting value involving register C has an exclusive-or operation with u,

A with t respectively.

$$C = ((C - S[2i + 1]) \ggg t) \oplus u$$

$$A = ((A - S[2i]) \ggg u) \oplus t$$

*Step*10. Repeat the *Step* 2 until all the rounds are decremented to 1

*Step*11. After completing the loop, D and B undergo a post-whitening.

$$D = D - S[1]$$

$$B = B - S[0]$$

V. RESULTS

The main aim of the project is to achieve node – node authentication between the sensor nodes and also to securely transfer the message which is generated in packets from the neighboring nodes to sink. For this process, the main function was divided into three phases namely, the key establishment phase which would establish a shared key for generation among the sensor nodes in the sensor network. The second phase consisted of the deployment phase where sensor nodes are deployed depending on the number of the nodes being inputted, the transmission range and the sensing range. The third phase consists of the event phase where the event is being processed by the node within its sensing range and generating the message in the form of packets to the sink node.

The final result obtained from these phases derives from the fact that key pre- distribution technique based on the LU matrix method achieves node to node mutual authentication which would have the benefits of greater network security, strong overhead, stronger resistance to faults or other related weaknesses and a better network resilience.

RC6 encryption and decryption algorithms have been used to protect the message of the data within the sensor nodes in the form of packets which have to be sent to the sink node where, it decrypts the message using the decryption algorithm. The purpose of using RC6 algorithm is its advantages are huge compared to other related security algorithms. The RC6 algorithm is a symmetric key block cipher which is derived from RC5 but is distinct from it in terms of its usage, its behavior and its functioning mechanism.

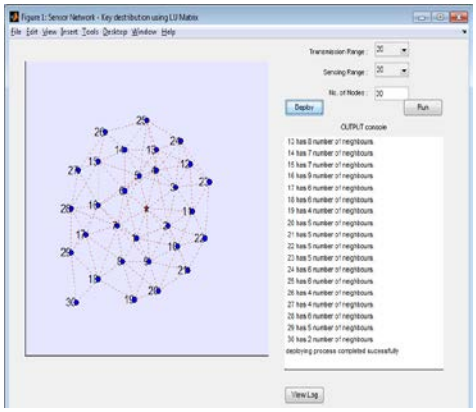

Fig 2. Figure identifying the number of neighbours in a sensor network

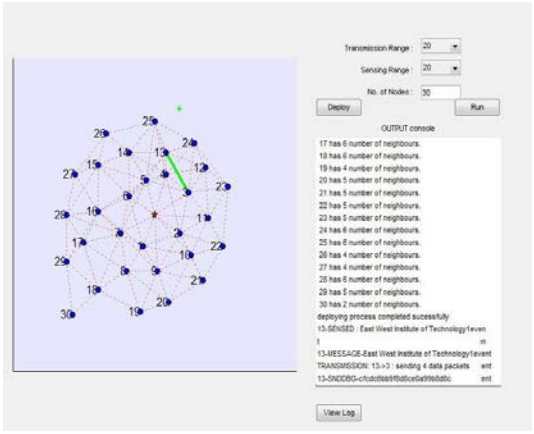

Fig 3. Figure showing the event generation and routing of data between nodes indicated by green light. The green point indicates the event sensed in the sensor network.

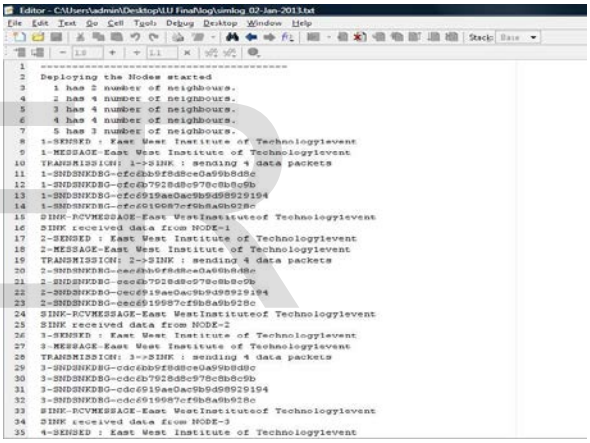

Fig 4. Figure showing the full description of the data flow from source to sink as well as the encryption and decryption technique used by event data.

CONCLUSION

In this paper, a new deployment and event processing technique was proposed. The existing key pre-distribution algorithm is presented for node to node mutual authentication and guarantees to find a common key between any two sensor nodes in the network. The routing of the data or message between the sensor nodes to the base station or sink is achieved through Djikstra's shortest path algorithm.

The RC6 encryption algorithm is used to secure data or message transmission between the sensor nodes.

RC6 encryption is similar to RC5 encryption algorithm but it has many advantages over the RC5 encryption algorithm.

Firstly, it uses integer multiplication, quadratic equation and fixed bit shifting for enhanced security. Secondly, its main design objective is its simplicity. Finally, it is so powerful that it is not reported to be vulnerable to any practical attacks thus making it one of the strongest methods to achieve secured node-node authentication in the sensor network.

The results which obtained demonstrate the proposed scheme provides the node to node secure data or message transmission without the loss of any data packets in the sensor network

ACKNOWLEDGMENT

The authors would like to thank the anonymous referees for their valuable comments, which greatly improved the readability of the paper.

REFERENCES

[1] L. Eschenauer and V. D. Gligor, "A key-management scheme for distributed sensor networks," In Proc. 9th ACM Conf. Computer Communication Security, New York, USA, 2002, pp. 41–47

[2] W. Du, J. Deng, Y. S. Han, P. K. Varshney, J. Katz, and A. Khalili, "A pairwise key predistribution scheme for wireless sensor networks," ACM Trans. Inf. System Security, vol. 8, no. 2, New York, USA, 2005, pp. 228–258. Conf. Computer Communication Security, New York, USA, 2002, pp. 41–47

[3] D. G. Liu, P. Ning, and R. F. Li, "Establishing pairwise keys in distributed sensor networks,"ACM Trans.Inf. System Security, vol. 8, no. 1, New York ,USA, 2005, pp. 41–77]

[4] D. Chakrabarti, S. Maitra, and B. Roy, "A key predistribution scheme for wireless sensor networks: Merging blocks in combinatorial design," in Proc. Lecture. Notes Computer Science, Springer, Berlin, 2005, pp. 89–103.

[5] Al-Sakib Khan Pathan, Tran Thanh Dai, and Choong Seon Hong, "An Efficient LU Decomposition-based Key Pre-distribution Scheme for Ensuring Security in Wireless Sensor Networks",

[6] Saurabh Singh#1, Harsh Kumar Verma *2, Tania Jain#3 "Pair-wise Key Establishment Scheme for Wireless Sensor Network Using LU Matrix", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 2 (4), USA, 2011, pp 1523-1528

[7] Key Predistribution Approach in Wireless Sensor Networks Using LU Matrix Hangyang Dai and Hongbing Xu, IEEE SENSORS JOURNAL, VOL. 10, NO. 8, AUGUST 2010, pp 1399-1402

[8] Morgan Monger, "RC6: The Simple Cipher", CS-627-0001: Cryptography Fall 2004

[9]William Stallings "Network Security Essentials",Application standards 3rd Edition, Pearson Education, ISBN 978-81-317-1664-9, 2009

[[10] Atul Kahate, "Cryptography and Network Security", 2nd Edition, ISBN – 13: 978-0-07- 064823-4, 2008