ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

A Two-Layer Key Scheme for Wireless detector Networks

K.G.S. Venkatesan[1], K.P.Kaliyamurthie[2]

[1]Assistant Professor, Department of Computer Science Engineering, Bharath University, Chennai, India

[2]Professor & Head, Department of Computer Science Engineering, Bharath University, Chennai, India

Abstract- In an oversized scale sensing element network, it's impracticable to assign a novel Transport Layer Key (TLK) for every try of nodes to produce the end-to-end security attributable to the large memory price per node. Thus, standard key establishment schemes follow a key predistribution approach to determine a Link Layer Key (LLK) infrastructure between neighboring nodes and admit multihop methods to produce the end-to-end security. Their drawbacks embrace vulnerability to the node compromise attack, massive memory price, and energy unskillfulness with in the key institution between neighboring nodes. In this paper we propose a novel key establishment scheme, called LAKE, for sensor networks. LAKE uses a t - degree trivariate symmetric polynomial to facilitate the establishment of both T - 6954 -LKs and LLKs between sensor nodes two-dimensional, wherever every node will calculate direct TLKs and LLks with some logically neighboring nodes and trust those nodes to indirect TLKs and LLKs with different nodes. Any 2 finish nodes will talk over a TLK on demand directly or with the assistance of only 1 intermediate node, which may be determined earlier. As for the LLK, LAKE is safer below the node compromise attack with a lot of less memory price than the standard solutions. Owing to the location-based LAKE is additionally energy economical in this every node has direct LLKs with most neighbors an excessive amount of energy on the indirect LLKs with neighbors through multihop routing.

Keywords : Transport Layer Key (TLK), Link Layer Key (LLK).

I. INTRODUCTION

Security has been drawing wide interest in the area of wireless sensor networks, which usually consist of thousands of resource-limited sensor nodes deployed in a designated area without any fixed infrastructure because of the network vulnerability to malicious attacks in unattended and hostile environments such as battlefield surveillance and homeland security monitoring. Under such circumstances, security services such as encryption and authentication are indispensable for guaranteeing the proper operation of sensor networks.

Key management is incredibly essential to security protocols as a result of cryptography and authentication services are supported the operations involving keys. one amongst the basic issues of key management is the way to established keys to shield connections between detector nodes. Generally, 2 types of connections is fashioned during a network. One is that the one-hop association between a combine of neighboring nodes [1]. Within the network stack, this one-hop association is managed by the link layer protocol. So, as to secure the link layer association, a shared Link Layer Key (called LLK hereafter) has to be established between the neighboring nodes. Theother style of association is fashioned between 2 nodes over a multihop path. as a result of the 2 nodes are out of every other's neighborhood, this end-to-end association is managed by the transport layer protocol rather than the link layer protocol. Therefore, a Transport Layer Key (called TLK hereafter) has to be established to produce the end-to-end security. The TLK institution isn't a straightforward drawback. In a network of N nodes, in theory, every node is preloaded with

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

N nine one keys unambiguously shared withdifferent nodes, however the feasibleness is challenged attributable to the contradictory needs between the scarce memory of detector nodes and also the massive scale of detector networks. Instead, most up-to-date solutions relax the protection demand and target the institution of Link Layer Keys (LLK) between any combine of neighboring nodes.
In a massive scale detector network, the quantity of neighbors of a node is typically at low constant. Thus, it's a lot of possible to determine Associate in Nursing LLK infrastructure by that to save lots of memory resource [3]. supported this LLK infrastructure, 2 finish nodes will perform secure communications over a multihop path with the assistance of intermediate nodes and might talk over a TLK on demand, if needed, through the secure handclasp. TheLLK infrastructure will effectively stop external attackers from accessing the network, however cannot counteract internal attackers, like compromised nodes. Therefore, a TLK negotiated on a multilink path is exposed if any of the intermediate nodes is compromised. as a result of the quantity of hops on a path is massive, the chance of the TLK exposure is quite high. Moreover,
The previous LLK schemes themselves also are liable to node compromise. Associate in resister will use the secrets in compromised nodes to derive the secrets shared between different noncommissioned officer secure nodes. Hence, some compromised nodes might cause several failure points within the network and destroy the whole LLK infrastructure. Another downside of the previous LLK theme is that they need an oversized memory demand to take care of an explicit level of security or property.

Based on our work, we have a tendency to introduce a unique theme, referred to as LAKE (two-Layer Key establishment), for the institution of each TLKs and LLKs in detector networks. notably, all detector nodes square measure organized into a two-dimensional area and a trivariate polynomial is decentralized to facilitate the TLKs and LLKs within the area. to extend property and scale back communication overhead, the nodes near one another square measure preloaded with correlative secrets, referred to as shares, derived from the trivariate polynomial. the most contributions **square measure** as follows:

- Compared with the standard LLK schemes, LAKE options abundant less memory price, which might be but, which can be less than 1:8171 $\sqrt{N}$, where N is the total number of nodes in the network.
- By utilizing location info, LAKE guarantees that 2 neighboring nodes will establish a right away LLK with high chance. This provides energy potency compared with the standard LLK schemes as a result of the chance of indirect LLK..

We describe LEAP (Localized Encryption and Authentication Protocol), We describe LEAP (Localized encoding and Authentication Protocol), a key management protocol for sensing element networks that's designed to support in-network process, whereas at constant time proscribing the safety impact of a node compromise to the immediate network neighborhood of the compromised node [4]. The look of the protocol is intended by the observation that differing types of messages changed between sensing element nodes have totally different security necessities, which one keying mechanism isn't appropriate for meeting these totally different security necessities.

LEAP supports the institution of 4 sorts of keys for every sensing element node a private key shared with the bottom station, a combine wise key shared with another sensing element node, a cluster key shared with multiple neighboring nodes, and a bunch key that's shared by all the nodes within the network. The protocol used for establishing and change these keys is communication- and energy-efficient, and minimizes the involvement of the bottom station. LEAP additionally includes associate economical protocol for native broadcast authentication supported the utilization of unidirectional key chains.

A salient feature of the authentication protocol is that it supports supply authentication while not precluding in-

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

network process. Our performance analysis shows that LEAP is extremely economical in computation, communication, and storage. we have a tendency to analyze the safety of LEAP below varied attack models and show that LEAP is extremely effective in defensive against several subtle attacks like howdy Flood attack, Sybil attack, and hole attack. A model implementation of LEAP in a very sensing element network test bed is additionally rumored. we've got conferred LEAP (Localized encoding and Authentication Protocol), a key management protocol for sensing element networks. LEAP has the subsequent properties:

• LEAP includes support for establishing four types of keys per sensor node – individual keys shared with the base station, pair wise keys shared with individual neighboring nodes, cluster keys shared with a set of neighbors, and a group key shared with all the nodes in the network. These keys can be used to increase the security of many non-secure protocols. LEAP includes an efficient protocol for local broadcast authentication based on the use of one-way key chains.

• A distinguishing feature of LEAP is that its key sharing approach supports in-network processing, while restricting the security impact of a node compromise to the immediate network neighborhood of the compromised node.

• LEAP can prevent or increase the difficulty of launching many security attacks on sensor networks.

• The key establishment and key updating procedures used by LEAP are efficient and the storage requirements per node are small. Our implementation indicates LEAP is feasible for the current generation sensor nodes.

II.EXISTING SYSTEM

Keymanagement is extremely important to security protocols as a result of secret writing and authentication services area unit supported the operations involving keys. one among the basic issues of key management is the way to originated keys to shield connections between device nodes. Generally, 2 types of connections are often fashioned in a very network. One is that the one-hop association between a try of neighboring nodes, within the network stack, this one-hop association is managed by the link layer protocol. so as to secure the link layer association, a shared Link Layer Key (called LLK hereafter) has to be established between the neighboring nodes [5]. the opposite kind of association are often fashioned between 2 nodes over a multihop path. as a result of the 2 nodes area unit out of every other's neighborhood, this end-to-end association is managed by the transport layer protocol rather than the link layer protocol. Therefore, a Transport Layer Key (called TLK hereafter)has to be established to produce the finish-to end security. The TLK institution isn't a simple drawback.

In a network of N nodes, in theory, every node are often preloaded with N - one keys unambiguously shared with different nodes, however the practicability a often challenged due to the contradictory necessities between the scarce memory of device nodes and also the giant scale of device networks. Instead, most up-to-date solutions relax the protection demand and target the institution of Link Layer Keys (LLK) between any try of neighboring nodes. In a giant scale device network, the quantity of neighbors of a node is typically alittle constant. Thus, it's a lot of possible to determine associate degree LLK infrastructure by that to avoid wasting memory resource. Supported this LLK infrastructure, 2 finish nodes will perform secure communications over a multihop path with the assistance of intermediate nodes and might talk terms a TLK on demand, if needed, through the secure acknowledgment. The LLK infrastructure will effectively stop external attackers from accessing the network, However cannot counteract internal attackers, like compromised nodes [6]. Therefore, a TLK negotiated on a multilink path are often exposed if any of the intermediate nodes is compromised. as a result of the quantity of hops on a path are often giant, the chance of the TLK exposure is quite high. Moreover, the previous LLK schemes themselves also are prone to node compromise. associate degree resister will use the secrets in compromised nodes to derive the secrets shared between different non compromised nodes. Hence, some compromised nodes could cause several failure points within the network and destroy the whole LLK infrastructure. Another downside of the previous LLK theme is that they need an oversized memory demand to keep up a definite level of security or property.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

III.PROPOSED SYSTEM

LAKE is more secure under the node compromise attack with much less memory cost than conventional solutions. Energy efficient in that each node has direct LLKs with most neighbors without spending too much energy on the establishment of indirect LLKs with neighbors through multihop routing.

Based on our work , we introduce a novel scheme, called LAKE (two-Layer Key Establishment), for the establishment of both TLKs and LLKs in sensor networks. Particularly, all sensor nodes are organized into a two dimensional space and a trivariate polynomial is predistributed to facilitate the establishment of TLKs and LLKs in the space [6]. To increase connectivity and reduce communication overhead, the nodes close to each other are preloaded with correlated secrets, called shares, derived from the trivariate polynomial. The main contributions are as follows:

- Our LAKE effectively addresses the TLK establishment problem for sensor networks. Any two nodes can negotiate a TLK on demand directly or with the help of only one intermediate node. Though, in conventional LLK schemes, two nodes can also negotiate a TLK through a multihop path, there is more than one intermediate node that can learn the TLK. Hence, LAKE is much more secure under the node compromise attack compared with conventional proposals.

- Compared with the conventional LLK schemes, LAKE features much less memory cost, which can be less than 1:8171 $\sqrt{N}$, where N is the total number of nodes in the network.
- By utilizing location information, LAKE guarantees that two neighboring nodes can establish a direct LLK with high probability. This provides energy efficiency compared with the conventional LLK schemes because the probability of indirect LLK

3.1 Advantages of Proposed System

- Energy efficient Energy efficient in that each node has direct LLKs with most neighbors without spending too much energy on the establishment of indirect LLKs with neighbors through multihop routing.
- To increase connectivity and reduce communication overhead
- More secure under the internal node compromise attack compared with conventional proposals.

IV.ARCHITECTURE OF SENSOR NETWORK SYSTEM

4.1 Sensor Network

A low-speed industrial network that is used to connect sensors to actuators. A sensor network implies limited or no controller functions. Multiple sensor networks may be coupled to form device networks..

4.2 Transport Layer

The transport layer is that the second highest layer within the four and 5 layer TCP/IP reference models, wherever it responds to service requests from the applying layer and problems service requests to the network layer. it's additionally the name of layer four of the seven layer OSI model, wherever it responds to service requests from the session layer and problems service requests to the network layer.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

4.3 Data Link Layer

The data link layer is layer 2 of the seven-layer OSI model likewise as of the five-layer TCP/IP reference model. It responds to service requests from the network layer and problems service requests to the physical layer. This is the layer that transfers knowledge between adjacent network in an exceedingly wide space network or between nodes on an equivalent native space network section. The link layer offers the purposeful and procedural suggests that to transfer data between network entities and presumably provide the suggests that to sight and possibly correct errors which will occur within the Physical layer. samples of circuit protocols area unit for native area networks and UPPP, HDLC and ADCCP for point-to-point connections.

4.4 Link Layer Key

Link-layer keys between neighboring nodes are a basic issue in securing detector network communications. Most existing solutions are key pre-distribution schemes that trust detector nodes to broadcast many or maybe thousands of preloaded key IDs to seek out pair wise keys between neighboring nodes. Link-layer keys between neighboring nodes could be a basic issue in securing detector network communications. Most existing solutions are key pre-distribution schemes which rely on sensor nodes to broadcast hundreds of or even thousands of preloaded key IDs to find pairwise keys between neighboring nodes.

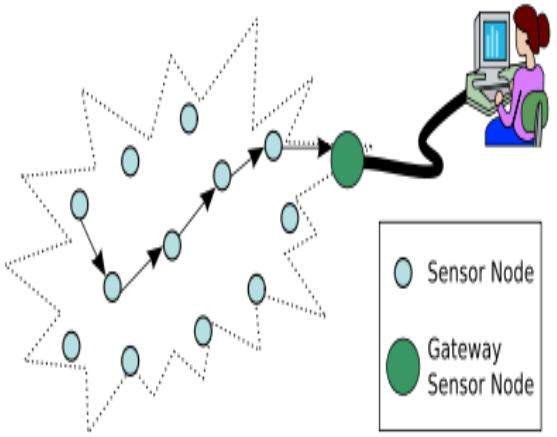

Fig-1 : Architecture of Wireless Sensor Networks

V. SYSTEM MODULES

5.1 Share Predistribution:

In this module, shares of a global t-degree trivariate polynomial are predistributed among sensor node. This polynomial is used to derive shares for sensor nodes. To establish keys, every node should have two credentials (1; c2) which are positive and pair wise different. These credentials can be created and preloaded into nodes before deployment [7]. However, it requires additional memory space per node in Figure 2. Fortunately, the two credentials can be derived from node ID by a bijection,

i.e. c1 = n1 + 1 + N2,
c2 = n2 + 1 where ni = 0; 1;. .; Ni _ 1 for i = 1, 2.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Thus, the two credentials are drawn from different zones [N2 + 1; N1 + N2] and [1, N2], respectively, which guarantee they are positive and pair wise different. Besides, by doing this mapping, each node needs to store only N2 instead of two credentials. Hence, every node in the network needs to keep only a t-degree univariate polynomial that has t + 1 coefficient over a finite field IFq. Those coefficients are preloaded into every node's memory before deployment and used to establish keys after deployment.

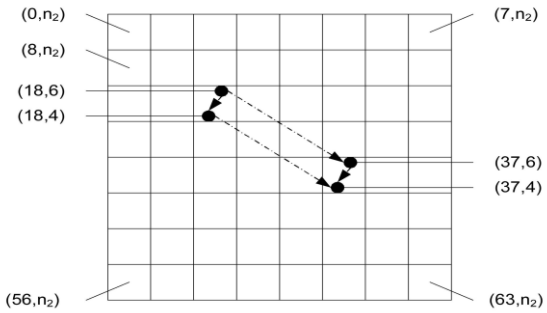

Fig-2 : Nodes at cell boundary in share

5.2 Direct key calculation:

All the shares cannot reveal the global polynomial even if they are captured by adversaries. Two nodes can calculate a shared key directly with the shares they hold if they are logical neighbors in the space. In this module, two nodes can calculate a shared key directly if they have a credential in common, i.e., a common index in their node IDs. We will call one of the two nodes a level-i neighbor of the other if their i^{th} indices in their IDs are different and the other indices are the same [8]. Obviously, every node can establish shared keys with its neighbors at level-1 (intercell) and level-2 (intracell). In the two-dimensional network, all nodes in each cell are level-2 neighbors because they have the same cell ID, and each node has a level-1 neighbor in each of other cells. For example, in the two-dimensional network in Fig. 1, node (18, 4) and node (18, 6) are level-2 neighbors and they can calculate a shared key directly. Node (18, 4) and node (37, 4) are level-1 neighbors and they can also calculate a shared key directly. All nodes can calculate direct keys on their own without interaction with other logical neighbors. Each direct key between two logical neighboring nodes is only secret to them. An adversary cannot learn the direct key unless he/she knows the corresponding polynomial share.

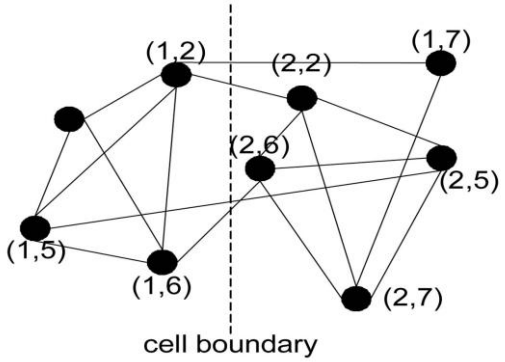

Fig- 3 : Nodes in cell boundary

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

5.3 Indirect key negotiation:

The indirect key negotiation section tells a way to hash out a shared key between 2 nodes with the assistance of another node if they're not logical neighbors. If 2 nodes don't have any common indices in their IDs, they can't calculate a shared key directly as a result of they are not logical neighbors. This happens once the 2 nodes reside completely different in several cells and that they have different indices in their cells, severally [9]. During this case, one node will notice in its cell a level-2 neighbor, that is additionally a level-1 neighbor of the opposite node. Then, the intermediate node will act as associate degree agent to facilitate a shared key negotiation between the 2 finish nodes. There are 2 agent nodes that may facilitate the indirect key negotiation. Suppose node u with ID (u1; u2) and node v with ID (v1; v2), wherever u1 not adequate to v1 and u2 not adequate to v2, ought to hash out a shared key. Either node (u1; v2) or node (v1; u2) will act as associate degree agent as a result of either one is that the common neighbor of nodes u and v. for instance, in Fig. 3 are 2 secure methods between node (18, 6) and node (37, 4) and a shared key are often negotiated through either of the secure methods with the assistance of the agent nodes (18,4) or (37,6).

5.4 TLK and LLK Establishment:

Due to the massive variety of nodes within the network, it's not possible to determine a TLK for every try of nodes and store the TLK within the try of nodes throughout the network data formatting part.[8] A dynamic of TLKs is extremely promising in large-scale sensing element networks. Generally, a TLK ought to be dynamically established on demand throughout the acknowledgement procedure between any try of nodes once they need to speak with one another. Like the LLK institution, every node will establish a right away TLK for every of the opposite nodes in its cell as a result of the level-2 neighbors. As every node includes a level-1 neighbor in every of alternative cells within the network, it will establish a right away TLK for the level-1 neighbor in this cell (like nodes (18,6) and (37,6) in Fig. 3). Then, it will deem the level-1 neighbor as associate agent to determine indirect TLKs with alternative nodes in this cell (in Figure 3) and node (18,6) will negociate associate indirect TLK with node (37,4) through node (37,6)). A prospect that node (37,6) isn't in cell thirty seven, however the underlying routing protocol will relay key negotiation messages between these nodes as is assumed in previous work. If a secure link is outlined because the communication path between 2 nodes that have a shared key, wherever the secure link could also be one-hop or multihop, LAKE can do the TLK agreement through a secure path consisting of no quite two secure links, which implies that at the most one agent is required to facilitate the TLK institution between any 2 finish nodes. every secure path in most standard schemes, that target LLK institution, sometimes consists of quite 2 secure links, and therefore the length of the secure path is troublesome to work out as a result of it depends on not solely the underlying routing protocol, however additionally the institution of direct keys between neighboring nodes, particularly in large-scale networks. Thus, most standard schemes are additional at risk of the node [10].

Given node density and radio radius in a very large-scale device network, the quantity of neighbors of a node is typically tiny. every node could establish LLKs for all neighbors and keep those LLKs in its memory for future use [11]. This could be done simply once node preparation as a result of every node has been preloaded with a polynomial share which may facilitate key institution. once 2 neighboring nodes square measure from identical cell, i.e., have identical cell index, they will apply the direct key calculation to ascertain associate degree LLK. as a result of the preparation information, will be given, expect that every node can establish LLKs directly with most of its neighboring nodes as a result of the virtually from identical cell. If 2 neighboring nodes square measure from totally different cells however the level-1 neighbors, then they will calculate an immediate LLK, a bit like nodes (1,2) and (2,2) in Fig. 2. albeit level-1 neighbors square measure distant from one another, like nodes (1,5) and (2,5), they will perpetually calculate a shared key severally. The keys between level-1 neighbors will act as bridgesbetween 2 cells. A node in one cell will undergo any of the bridges to barter keys with nodes within the alternative cell. In Fig. 2,for instance, node (1,2) will discuss associate degree indirect LLK with node (2,6) through either node (2,2) or node (1,6).Due to the preparation error, some nodes could reside outside of their supposed cells. In Fig. 2, for instance, node (1,7) must establish LLKs with neighboring nodes (2,2), (2,5), and (2,6) during this case, node (1,7)will perform indirect

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

key negotiation through its level-1 neighbor (2,7) Of course, node (2,7) is also a multihop faraway from node (1,7), however the underlying routing protocol will route key negotiation messages between them, just as is .Communication overhead may be a concern within the indirect LLK negotiation. LAKE includes preparation info into the institution of LLKs, thus, every node could calculate direct LLKs with the majority of its neighbors [9]. This high native secure property is fascinating as a result of it implies that every node doesn't have to be compelled to pay an excessive amount of energy on the institution of indirect LLKs with neighbors through multihop routing. typical LLK schemes with uniform key predistribution have additional energy consumption in terms of lower native secure property, we are going to measure the secure property assumptive Gaussian distribution for node location in every cell [12].

VI.TESTING

6.1 Test Data and Output

Unit Testing:

Unit testing is conducted to verify the functional performance of each modular component of the software. Unit testing focuses on the smallest unit of the software design (i.e.), the module.[9] The white-box testing techniques were heavily employed for unit testing.

Functional Tests:

Functional test cases involved exercising the code with nominal input values for which the expected results are known, as well as boundary values and special values, such as logically related inputs, files of identical elements, and empty files.[10]

Three types of tests in Functional test:

- Performance Test
- Stress Test
- Structure Test

Structured Test:

- Exercise all logical decisions on their true or false sides.
- Execute all loops at their boundaries and within their operational bounds.
- Exercise internal data structures to assure their validity.

6.2 Testing Techniques / Testing strategies :

Testing is a process of executing a program with the intent of finding an error. A good test case is one that has a high probability of finding an as-yet –undiscovered error. A successful test is one that uncovers an as-yet- undiscovered error. [11] System testing is the stage of implementation, which is aimed at ensuring that the system works accurately and efficiently as expected before live operation commences. It verifies that the whole set of programs hang together. System testing requires a test consists of several key activities and steps for run program, string, system and is important in adopting a successful new system. This is the last chance to detect and correct errors before the system is installed for user acceptance testing.[12]

Basis path testing:

- Flow graph notation
- Cyclometric complexity
- Deriving test cases

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

- Graph matrices Control

Black Box Testing:

The steps involved in black box test case design are:

- Graph based testing methods
- Equivalence partitioning
- Boundary value analysis
- Comparison testing

6.3 SOFTWARE TESTING STRATEGIES

A software testing strategy provides a road map for the software developer. Testing is a set activity that can be planned in advance and conducted systematically.[13] For this reason a template for software testing a set of steps into which we can place specific test case design methods should be strategy should have the following characteristics:

- Testing begins at the module level and works "outward" toward the integration of the entire computer based system.
- Different testing techniques are appropriate at different points in time.

System Security Measures:

System security refers to the technical innovations and procedures applied to the hardware and operating systems to protect against deliberate or accidental damage from a defined threat.

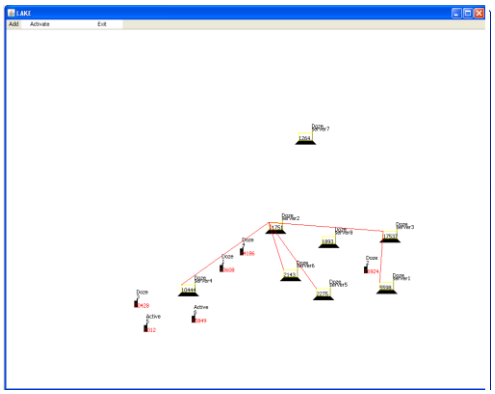

Figure 4 : Different LAKE node Structure

- Physical securities are production from fire flood and other physical damage.
- Database integrity through data validation techniques.

Password is the most common authentication mechanism based on sharing of secret. In a password –based system each user has a password, which may initially be assigned by the system or an administrator.[14] In Online Recruitment System, only administrator is allowed to change the users passwords. The system stores all users passwords and users them to authenticate the user. When logging in, the system request the user supplies a presumably secret, user specific password. This way the passwords provide protection to some extent The proper backup of data in the form of hardcopies as well as on paper stationary is a measure of disaster recovery planning. [15]

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

Database / Data security:

The design of database involved to maintain various security levels to maintain the data in table.

- Data Integrity
- Primary Key
- Unique Key
- Not null

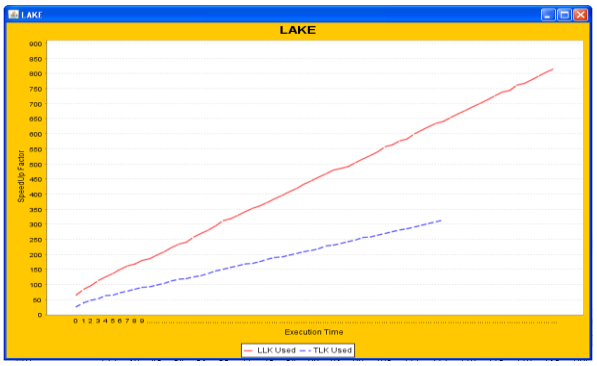

Figure 5 : Execution time & Speedup factor of LAKE

VII.FUTURE ENHANCEMENT

An authentication protocol that uses certificates containing an asymmetric key and a multilayer key architecture so that the (control cluster head) CCH is achieved using the threshold scheme, thereby reducing the computational overhead and successfully defeating all identified attacks. Our implementation indicates LAKE is feasible for the current generation sensor nodes.[16]

Each node does not need to spend too much energy on the establishment of indirect LLKs with neighbors through multihop routing. Conventional LLK schemes with uniform key predistribution have more energy consumption in terms of lower local secure connectivity., we will evaluate the secure connectivity assuming Gaussian distribution for node location in each cell. [17]

VIII.CONCLUSION

LAKE uses a t-degree trivariate polynomial to facilitate the key establishment between sensor nodes in a two-dimensional space. It can efficiently establish both TLKs and LLKs in sensor networks. Any two nodes can negotiate a TLK with the help of no more than one intermediate node. As for the LLK establishment, LAKE is more secure under the node compromise attack with much less memory cost than conventional schemes. The direct keys with almost all neighbors and does not need to consume too much energy on the establishment of indirect keys with neighbors through multihop routing, thus saving significant communication overhead.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

IX.ACKNOWLEDGMENT

The author would like to thank the Vice Chancellor, Dean-Engineering, Director, Secretary, Correspondent, Principal, HOD of Computer Science & Engineering **Dr. K.P. Kaliyamurthie**, Bharath University, **Chennai** for their motivation and constant encouragement. The author would like to specially thank to **Dean CSE Dr. A. Kumaravel** for his guidance and for critical review of this manuscript and for his valuable input and fruitful discussions in completing the work and the Faculty Members of Department of Computer Science & Engineering. Also, he takes privilege in extending gratitude to his parents and family members who rendered their support throughout this Research work.

REFERENCES

1. I.F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A Survey on sensor Networks," IEEE Comm. Magazine, Vol. 40, No. 8, pp. 102-114, Aug. 2002.
2. S. Sathish Raja and K.G.S. Venkatesan, "Email spam zombies scrutinizer in email sending network infrastructures", International journal of Scientific & Engineering Reseach, Vol. 4, Issue 4, PP. 366 – 373, April 2013.
3. Kamatchi P., Selvaraj S., Kandaswamy M., "Synthesis, magnetic and electrochemical studies of binuclear copper(II) complexes derived from unsymmetrical polydentate ligands", Polyhedron, ISSN : 0277-5387, 24(8) (2005) PP.900-908.
4. J.M. Kahn, R.H. Katz, and K.S.J. Pister, "Next Century Challenges: Mobile Networking for Smart Dust," Proc. MobiCom, pp. 217-278, Aug. 1999.
5. G.J. Pottie and W.J. Kaiser, "Wireless Integrated Network Sensors," Comm. ACM, vol. 43, no. 5, pp. 51-58, May 2000.
6. Babu T.A., Joseph N.M., Sharmila V., "Academic dishonesty among undergraduates from private medical schools in India. Are we on the right track?", Medical Teacher, ISSN : 0142-159X, 33(9) (2011) PP.759-761.
7. K.G.S Venkatesan and M.Elamurugaselvam, "Using the conceptual cohesion of classes for fault prediction in object-oriented system", International journal of Advanced & Innovative Research, Vol. 2, Issue 4, pp. 75 – 80, April 2013.
8. Suresh V., Jaikumar S., Arunachalam G., "Anti diabetic activity of ethanol extract of stem bark of Nyctanthes arbor-tristis linn", Research Journal of Pharmaceutical, Biological and Chemical Sciences, ISSN : 0975-8585, 1(4) (2010) PP.311-317.
9. H. T. Kung and D. Vlah, "Efficient Location Tracking Using Sensor Networks",
Proc. IEEE Wireless Comm. and ntworking Conf. (WCNC '03), Mar. 2003.
10. Sayeed and P. Ramanathan,, "Distribute Targetation Classification and Tracking in Sensor Networks," Proc. IEEE, Vol. 91, no. 8, pp. 1163-1171, 2003.
11. Singamsetty P., Panchumarthy S., "Automatic fuzzy parameter selection in dynamic fuzzy voter for safety critical systems", International Journal of Fuzzy System Applications, ISSN : 1562-2479 , 2(2) (2012) PP. 68-90..
12. K.G.S. Venkatesan and M.Elamurugaselvam "Design based object oriented Metrics to measure coupling & cohesion", International journal of Advanced & Innovative Research, Vol. 2, Issue 5, pp. 778 – 785, 2013.
13. A. Wood and J. Stankovic, "Denial of Service in Sensor Networks," IEEE Computer Magazine, vol. 35, no. 10.
14. Kiran B., Kareem S.A., Illamani V., Chitralekha S., "Case of Phthiriasis palpebrarum with blepheroconjunctivitis", Indian Journal of Medical Microbiology, ISSN : 0255-0857, 30(3) (2012) PP. 354-356..
15. K.G.S. Venkatesan, "Comparison of CDMA & GSM Mobile Technology", Middle-East Journal of Scientific Research, 13 (12), PP. 1590 – 1594, 2013.
16. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. First IEEE Int'l Workshop Sensor Network Protocols and Applications (SNPA '03), May 2003.
17. K.P.Kaliyamurthie, R. Udayakumar, and D. Parameswari, "Highly Secured Online Voting System over Network". Indian Journal of Science and Technology, Volume 6(6S), PP:4831-4836, June 2013. ISSN : 0974-6846.
18.Dr.A.Muthu Kumaravel, KNOWLEDGE BASED WEB SERVICE, International Journal of Innovative Research in Computer and Communication Engineering, ISSN(Online): 2320-9801,pp 5881-5888, Vol. 2, Issue 9, September 2014
19.Dr.A.Muthu Kumaravel, Data Representation in web portals, International Journal of Innovative Research in Computerand Communication Engineering, ISSN(Online): 2320-9801,pp 5693-5699, Vol. 2, Issue 9, September 2014
20.Dr.Kathir.Viswalingam, Mr.G.Ayyappan,A Victimization Optical Back Propagation Technique in Content Based Mostly Spam Filtering ,International Journal of Innovative Research in Computerand Communication Engineering ,ISSN(Online): 2320-9801 , pp 7279-7283, Vol. 2, Issue 12, December 2014

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 8, August 2015

21.KannanSubramanian,FACE ECOGNITION USINGEIGENFACE AND SUPPORT ECTORMACHINE,International Journal of Innovative Research in Computerand Communication Engineering,ISSN(Online): 2320-9801,pp 4974-4980, Vol. 2, Issue 7, July 2014.
22.Vinothlakshmi.S,To Provide Security & Integrity for StorageServices in Cloud Computing ,International Journal of Innovative Research in Computer and Communication Engineering ,ISSN(Online): 2320-9801 , pp 2381-2385 ,Volume 1, Issue 10, December 2013