3. System Architecture

The general definition of PKI is that it is a set of hardware, software, people, policies, and procedures need to generate, supervise, allocate, utilize, store up, and revoke certificates. In the proposed system each and every node has their public and private key, after the broadcast each genuine node has public key of each node present in the network. As shown in the Fig. 2 there nu of genuine node and replica node also present. Each node contain its own public and private key, it also contains the public key of others. The steps of algorithm and the mathematical module shown in the next section.

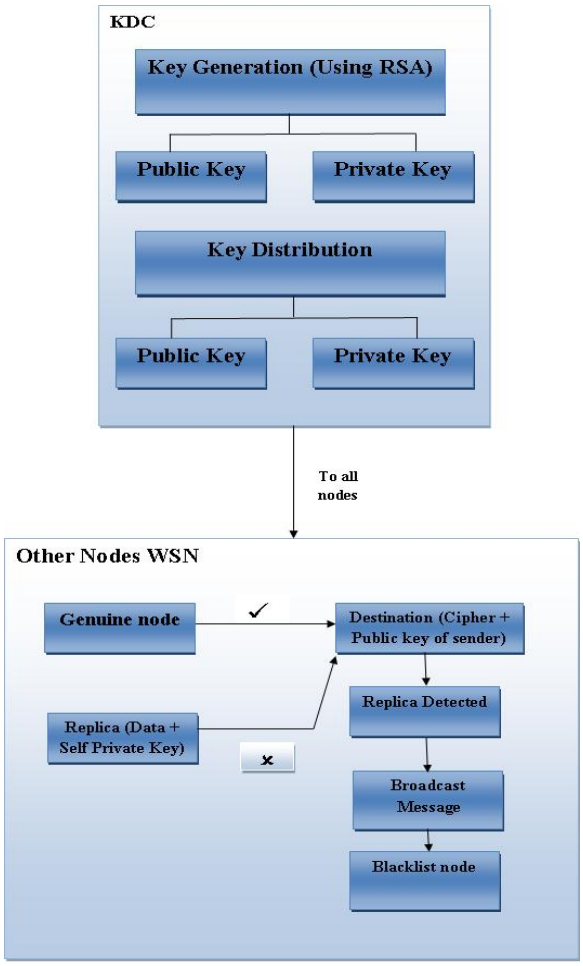


Figure 2: System architecture of proposed method

4. Performance Evaluation

a. PKI Algorithm

The steps of the proposed algorithm are as follows:

1. The public key and private key are distribute to the each and every sensor node in the network.
2. The public key of all the nodes are distributed to each other.
3. The genuine node A sends the encrypted data to the destination node B. B decrypts data by its own public key.
4. C is the replica of A. C behaves like A. C sends the data encrypted by its own private key to B.
5. B tries to decrypt the data by A's public key but fails to decrypt.
6. B tries to decrypt the data by all nodes public key
7. Data decrypted by C's public key.
8. Then it is detected that C is the replica of A

b. Mathematical Model

Mathematical consist of three sections Key Generation, Encryption and Decryption.

1. Key Generation

As we know that PKI contains public and private key. Public key is distributed to everyone in the network and it is used for encrypt the message. The keys for this algorithm are generated as follows:

Select any two prime numbers x and y.

These numbers are choose for security purpose and should be of similar bit length. The equation for primary number is as follows:

$$\text{Calculate } v = xy$$

Where v is the modulus for primary and public key and its length shown in bits. 'a' is the term as the public key exponent. 'b' is kept as private key exponent.

2. Encryption

Node A sends his public key to node B and takes private key secret. B requested node A to send message. Then A encrypts the message. The general equation of encrypt the message is as follows:

$$C = d^a \pmod v$$

Where C is the cipher text converted message and d is the integer value of the original message.

3. Decryption

Now node B want to decrypt the message send by node A. Node B decrypt the message by the following equation.

$$d = C^b \pmod v$$

5. Implementation Details

1) Modules

The proposed application is implemented in the following environment

- **Simulation Set**: The application is implemented with the help of java language. Jung libraries are used for the network topology. For generating the sensor nodes and networks the Jung libraries are used.
- **Network**: In the proposed, we built a network system were nodes are organized in a topology used for implementation and simulation. These nodes are dynamically loaded.

There are mainly modules of the proposed system. The introductions of these four modules are as follows:

1) Network Creation

The mobile sensor networks are generated for the implementation and simulation of proposed work. The network contains numbers of sensor nodes and connecting edges. The Jung tool is used for that. The nodes or the network are dynamically loaded.

2) Key Generation

The public key and private key are generate for all the sensor nodes present in the sensor networks. For generating the keys the above mention algorithm is used.

3) Key Distribution

After generating the public and private key for each sensor nodes in the network. The public of each node are distributed to the other nodes present in the network. The key was distributed for the purpose of encryption and decryption.

4) Communication using distributed keys

After generating and distributing the keys, the communication between the nodes is done. The sender sends the encrypted data to the destination node. There are numbers of nodes present in the network. Receiver receives the data and decrypts the data successfully by using the keys.

5) Attack Detection

The last phase is attacker detection. Our main aim of the proposed work is to detect the clone node and replica node. If the data receives by the node and decrypt successfully then it is genuine node. If the data received by the node and data is not decrypt by the senders public key at that time attackers are exist in the network. And the destination node try to find the attacker by decrypting the data by all the public keys.

2) Hardware Requirement

- Hard disk : 80 GB
- RAM : 512 MB
- Processor : Intel Pentium4 or above

3) Software Requirements

A. JAVA

The technology used for designing and implementation of this project is java as a coding language. We use the vector class for implementing the algorithm. The `Vector` class implements a grow able array of objects. Like an array, it contains components that can be accessed using an integer index. However, the size of a `Vector` can grow or shrink as needed to accommodate adding and removing items after the `Vector` has been created. Each vector tries to optimize storage management by maintaining a `capacity` and a `capacity Increment`. The `capacity` is always at least as large as the vector size; it is usually larger because as components are added to the vector, the vector's storage increases in chunks the size of `capacity Increment`. An application can increase the capacity of a vector before inserting a large number of components; this reduces the amount of incremental reallocation. For the GUI designing uses the swing class. For designing frames used jLabel, jTextFeildInputFile, jButtonBrows, jScrolPane, jButton object are used.

B. NetBeans IDE

NetBeans IDE are installed for implementing the java code. NetBeans is an integrated development environment (IDE) for developing primarily with Java, but also with other languages, in particular PHP, C/C++, and HTML5. It is also an application platform framework for Java desktop applications and others. The NetBeans IDE is written in Java and can run on Windows, OS X, Linux, Solaris and other platforms supporting a compatible JVM.

C. Jung Tool and Library for Forming Networks on the Frame.

Java Universal Network/Graph Framework is a software library, which is used for visualization, analysis the data which is represented as a graph or network. It is written in java. It is used to design directed or undirected graph, graph with parallel edges, multi-model graph etc. It also implements number of algorithms of graph theory, data mining, social network analysis such as optimization, decomposition, random graph generation, flows, etc. it is designed for to support the variety of representations of entities and their relations. It is also provide a visualization framework that makes it easy to construct the tools for the interactive exploration of network data. It is an open-source library; JUNG provides a common framework for graph/network analysis and visualization.

4) Network Model

In the proposed network model, here we form a tree network model in which contain root node which is also called as parent node and next is child node. The end nodes also called as leaf nodes. In tree network model contains different levels like level 1; level 2, etc depend on network model. In network may contain nodes which are denoted as a router, hubs, switches etc in the network. It also contains edges which are represented as a link in a network model. This network model is dynamically loaded and also we assign a weight to the each edge.

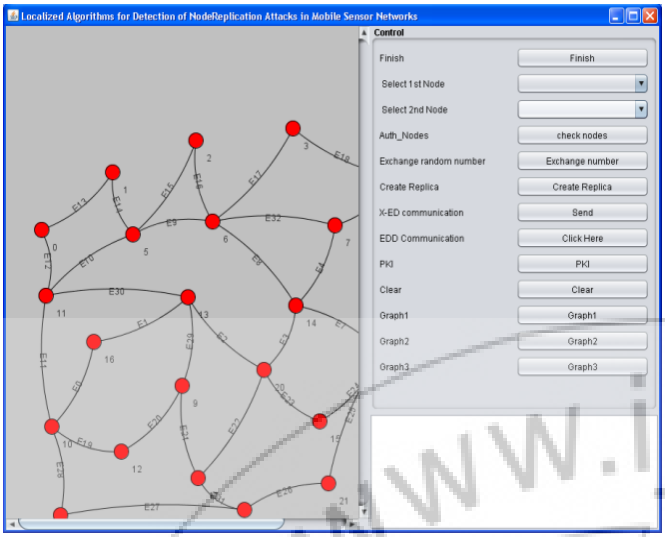
5) Simulation

After building tree, we enter a sink node. After that we get a shortest path which is generated by the multipath routing table. And it is used by the cluster head to forward the data towards the sink. Next, we enter the name of the cluster node. After entering the cluster node the cluster will be form. In which contain cluster head which is elected on the basis of highest residual energy and which is closer to the sink node. And remaining nodes which are also called as cluster members. The cluster member forwarded there data to the cluster head and cluster head aggregates this data with own data and after that it calculate the distance between two nodes. The cluster head select the shortest path which is generated by the multipath router and send this aggregate data to the sink. This algorithm shows that this will be help in fast construction, effective energy and dependable WSN applications. And also shows that our approach solution gives outperformance in different situations and in different key characteristics needed by WSNs.

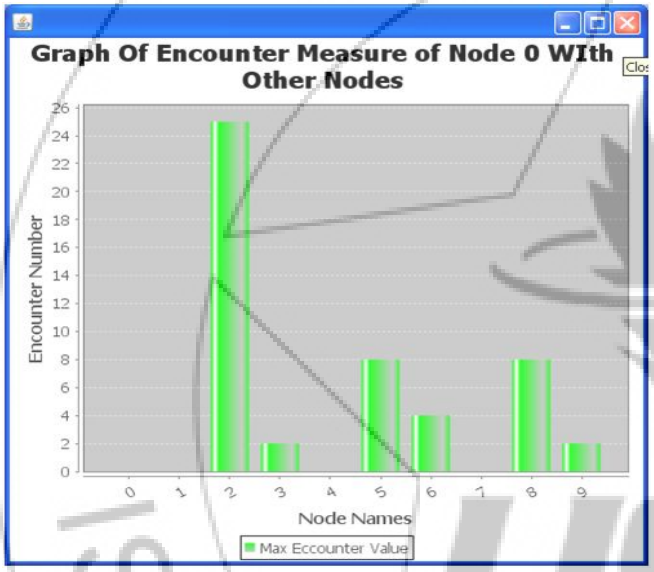
6. Results

As comparing with the existing system the simulation result of the proposed work is as follows:

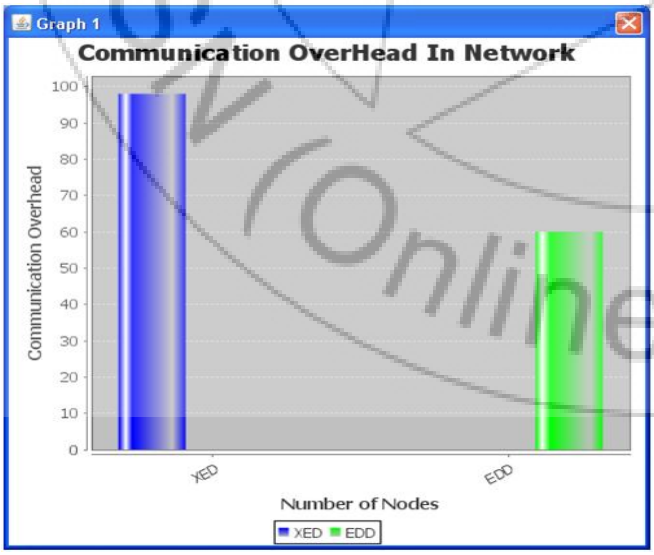
The existing algorithm trying to find the replica nodes but all the existing systems has some disadvantage as we discussed above. The proposed system detects the attacker node frequently with the exact location and with the real identity of the attacker node. After the simulation the following graphs shows the implementation result. We will show the two graphs in the result



Graph 1: Proposed method implementation window



Graph 2: Graph of Encounter Measure of Node 0 with Other Node



Graph 3: Communication Overhead in Network

7. Conclusion

In the proposed work we overcome the problem faced in the existing methods of localized algorithm for detecting node replication attack. In the proposed system as discussed above we used the public key infrastructure for detecting node replication attack on the mobile sensor network. The existing system like challenge response based method gives the solution for the problem faced during the detecting attack. We successfully detect the replication with high frequency with the help of PKI method.

8. Acknowledgement

I take this opportunity to extend my deep sense of gratitude and words of appreciation towards those who helped me during the pursuit of my present study. It gives me great pleasure and satisfaction to express my deep sense of gratitude towards my Post Graduate Guide Mr. .R.P. Kulkarni for accepting me as his student and gave me immense support during this Seminar work from beginning to end, in spite of his very busy schedule. I feel extremely fortunate to have him as my guide. My sincere thanks to Mr. Chaudari Sir P. G. coordinator, Prof. T. J. Parvat HOD CE Dept., Dr.M.S.Gaikwad Principal, S IT, Lonavala.

9. Future Scope

This work can be further extended to detect node replication attack with additional constraints such as QoS Parameters, Fault Tolerance.

References

[1] M. Conti, R. Di Pietro, L. V. Mancini, and A. Mei, *A randomized, efficient, and distributed protocol for the detection of node replication attacks in wireless sensor networks*, Proc.in Proc. ACMInt. Symp. Mobile Ad Hoc Networking and Computing (Mobi-Hoc), Montreal, Canada, 2007,

[2] Chia-Mu Yu, Yao-Tung Tsou, Chun-Shien Lu, *Localized Algorithms for Detection of Node Replication Attacks in Mobile Sensor Networks* , Proc. IEEE, and Sy-Yen Kuo, Fellow, IEEE

[3] B. Zhu, S. Setia, S. Jajodia, S. Roy, and L.Wang, *Localized multicast: Efficient and distributed replica detection in large-scale sensor networks* , IEEE Trans. Mobile Comput., vol. 9, no. 7, pp. 913.926, Jul. 2010.

[4] Y. Zeng, J. Cao, S. Zhang, S. Guo, and L. Xie, *Random-walk based approach to detect clone attacks in wireless sensor networks*, IEEE J.Sel. Areas Commun., vol.28, no. 5, pp. 677.691, Jun. 2010.

[5] M. Zhang, V. Khanapure, S. Chen, and X. Xiao *Memory efcient protocols for detecting node replication attacks in wireless sensor networks* , .Proc. IEEE Int. Conf. Network Protocols (ICNP), Princeton, NJ, USA, 2009, pp. 284.293

[6] R. Sarkar, X. Zhu, and J. Gao, *Double rulings for information brokerage in sensor networks*, In IBM Systems Journal,pages 335.352, 2006.

[7] K. Xing, F. Liu, X. Cheng, and D. Du *Real time detection of clone attack in wire- less sensor networks,.* , Proc. IEEE Int. Conf. Distributed Computing Systems (ICDCS), Beijing, China, 2008

[8] R. Brooks, P. Y. Govindaraju, M. Pirretti, N. Vijaykrishnan, and M. T. Kandemir *On the detection of clones in sensor networks using random key predistribution*, IEEE Trans. Syst., Man, Cybern. C, Applicat. Rev., vol. 37, no. 6, pp. 1246.1258, Nov. 2007.

[9] H. Choi, S. Zhu, and T. F. La Porta*SET: Detecting node clones in sensor networks,." in Proc. Int. ICST Conf. Security and Privacy in Communication Networks (Securecomm), Nice*, Proc. France, 2007, pp. 341.350.

[10] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo, *Mobile sensor network resilient against node replication attacks* , Proc.IEEE Conf. Sensor, Mesh, and Ad Hoc Communications and Networks (SECON), California, USA, 2008, pp. 597.599, (poster).

[11] C.-M. Yu, C.-S. Lu, and S.-Y. Kuo *Efcient and distributed detection of node replication attacks in mobile sensor networks* , Proc. IEEE Vehicular TechnologyConf. Fall (VTC-Fall), Anchorage, AK, USA, 2009, pp. 1.5

[12] J. Ho,M.Wright, and S. K. Das, , *Fast detection of replica node attacks in mobile sensor networks using sequential analysis* , IEEE Int. Conf. Computer Communications (INFOCOM), Brazil, 2009, pp. 1773.1781.

[13] K. Xing and X. Cheng *From time domain to space domain: Detecting replication attacks in mobile ad hoc networks* Proc. IEEE Int. Conf. Computer Communications (INFOCOM), San Diego, CA, USA, 2010, pp. 1.9

Author Profile

Mrs. H. B. Kadam was born in 1984.She received engineering degree in computer from Pune University. Completed her MBA from YCMOU university. Currently Pursuing ME in computers from Pune University. Presently she is working as an lecturer at AISSM's Polytechnic, Pune, Maharashtra, India