RESEARCH ARTICLE OPEN ACCESS

Enhanced Three Tier Security Scheme for Data in Network

Nikita J. Kulkarni[1], Prashant Erande[2], Neelima Jadhav[3]

Department of Computer Science and Engineering,
ZES's Dnyanganga College of Engineering And Research, Pune,
Maharashtra, India

ABSTRACT

In Three Tier Architecture, access nodes, act as authentication access points to the network, to detect the Data prov nodes to transfer their aggregated data to data req. A node sends data request messages to the Data prov nodes via a access node. These data request messages will initiate the stationary access node to detect data prov nodes, which transmit their data to the req node. Using two separate key pools and having few data prov nodes that carry keys from the Requester key pool will make it more difficult for the attacker to launch a data req node replication attack on the network by capturing only a few arbitrary data prov nodes. This scheme is divided into two stages: static and requester polynomial pre-distribution and key discovery. Also for access node replication attack, we will use a 1-way hash chain algorithm in conjunction with the polynomial pool scheme. In addition to the static polynomial, a pool of randomly generated passwords is used to enhance the security.

Keywords:- Data Req , Data prov, key pre-distribution, 1 -way hash chain algorithm

I. INTRODUCTION

The Three Tier Security Scheme is basically used for increasing the security of the system. Pair wise key distribution service is provided by the system to the normal user for password authentication. Two separate polynomials such as requester polynomial pool and static polynomial pool where the keys are stored and from these pools pair wise keys are picked randomly by data req and data prov. Due to which network security is improved. Replication attack to data prov is reduced. So our aim is to provide the normal users with a simple and secure data transfer. To secure the three tier network architecture from node replicated attack using two separate key pools, one for the Data req node to access the network, and one for pair wise key establishment between the Data prov; Also stationary access node replication attacks, using authentication mechanism between the Data prov and the stationary access node.

II. RELATED DATA

The key distribution [3] problem is an active research area in wireless networks. The main concept is to pick a set of keys from key pool by data prov node so that any two data prov nodes share at least one common key. This idea is further extended to two key pre distribution schemes [3]: the random pair wise keys scheme [4] and the q-composite key pre distribution scheme. The q-composite key pre distribution scheme also used a key pool, but required two data prov nodes to compute a pair wise key from at least q pre distributed keys that they shared. The random pair wise keys scheme randomly picked pairs of data prov nodes and assigned each pair a unique random key. Both schemes improved the security over the basic probabilistic key pre distribution scheme.

III. THREE TIER SECURITY SCHEME

In the proposed scheme, we use two separate polynomial pools: the Data req polynomial pool and the static polynomial pool. Polynomials from the Data req polynomial pool are used to establish the security between Data req and stationary access nodes, which will enable this Data req to access the Data prov for data collection. Thus, an attacker would compromise at least a single polynomial from the Requester polynomial pool to obtain access to the network for the data collection. Polynomials from the static polynomial pool are used to as certain the authentication and keys setup between the Data prov and stationary access nodes. Priority wise, each Data req randomly picks a subset of polynomials keys from the Requester polynomial pool.

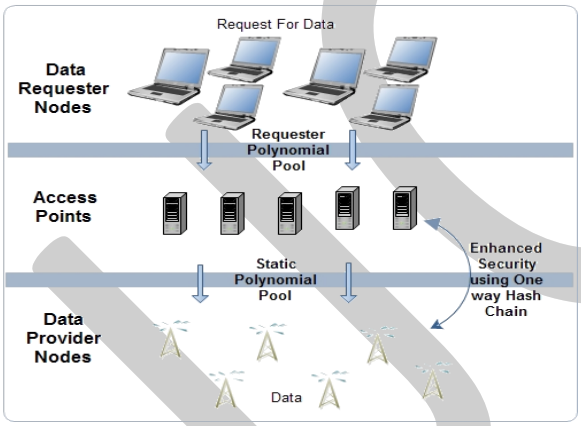

Figure 1: System Architecture

In this scheme, to improve the network security to Data req replication attack as compared to the single polynomial pool based approach, we intend to minimize the probability of a Data req polynomial being compromised if Data prov captured.

IV. ONE WAY HASH CHAIN ALGORITHM

In many security applications one-way chains are an important cryptographic primitive. As one way chains are very efficient to verify, they are recently becoming increasingly popular for designing security protocols as one way function can compute their low-powered processors within milliseconds. Two new concepts for one-way hash chains are introduced in this paper which significantly improves the efficiency of one way chains. The first construction, the Sandwich-chain, efficiently does verification of one way chain values if the trusted chain value of one way is far away and smaller bandwidth for one-way chain values is provided. Our second construction, Combo Skip chain, features a new lower bound for one-way chains in terms of storage and traversal overhead.

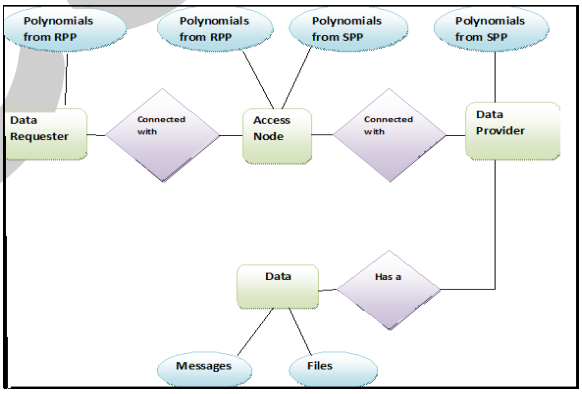

Figure 2: System Flow

Algorithm

Notation: Data prov – **u**; Data req node –**v;** Stationary Access Node- **a**

A) Stage I

1. Generate Requester Polynomial Pool called **M** of size |M|

2. Generate Static Polynomial Pool called **S** of size |S|

3. Randomly give K_m (K_m >1) from **M** to each **v**

4. Randomly give **1** polynomial from **M** to each **a**

5. Randomly give subset of K_s from **S** to each **u**

6. Randomly give (K_s -1) from **S** to each **a**

B) Stage II

7. **u** finds **a** such that; **a** can establish pair wise key with both **v & u**

If (**direct key establishment**)
{

1. **v** sends K_c (encrypted using K_{va}) to **a**
2. **a** receive message & share pair wise key with **u**
3. **a** sends K_c (encrypted using K_{au}) to **u**

}
Else
{

1. Find the intermediate data prov node.
2. Establish pair wise key with help of intermediate data prov node.
3. Establish direct communication using other data prov node.

}

C) 8. Using secure key pair establishment data req can request data from data prov node.

V. DESCRIPTION

In our system, system will ask user to login by entering the details. After login into the system the user will enter how much number of nodes is required i.e. data req nodes, data prov nodes and stationary access nodes to construct the three tier architecture. User will manually enter the number of nodes.

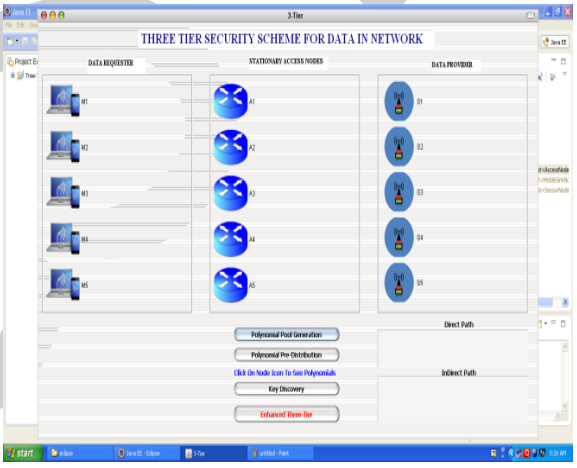

Figure 3:- Structure of System

After entering the number of nodes the three tier architecture is created as shown in figure 3.In above figure user has entered five data req nodes, five stationary access nodes and five data prov nodes.

Following are the operations used for constructing the path from data req node to data prov node through stationary access node:

Polynomial Pool Generation

Polynomial Pre-Distribution

Key Discovery

Enhanced Three-Tier

In above figure it also shows two panels below which display the direct and indirect path between data req node and data prov.

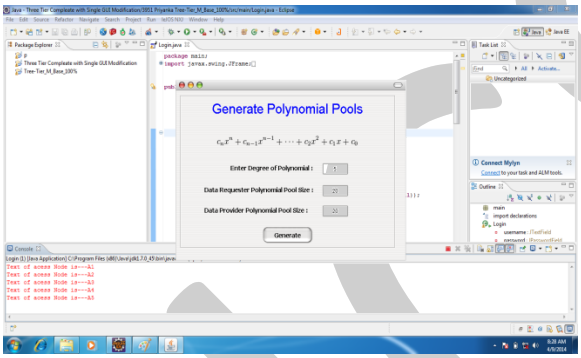

Figure 4:- Generation of Polynomial

For the generation of the polynomials binomial expression is used as shown in above figure.In which user is asked to enter the degree of polynomial,size of requester pool and static pool.These binomial expression produces number of keys or polynomials randomly.

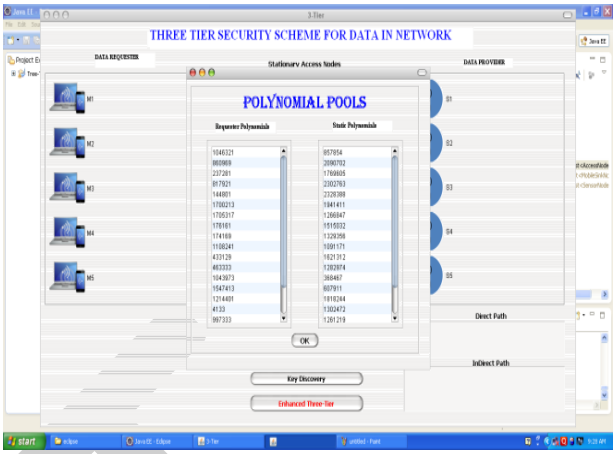

Figure 5:- Polynomial Pools

As described in above section, system contain two pools i.e. requester polynomial pool and static polynomial pool.These pool contain polynpmials or keys.Keys from requester polynomial pool are distributed to data req nodes and access nodes.Keys from static polynomial pool are distrbuted to access nodes and data prov nodes. Keys are randomly given K_m (K_m >1) from requester pool to each data req. Keys are randomly given 1 polynomial from requester to each access nodes. Keys are randomly given subset of K_s from static pool to each data prov. Keys are randomly given (K_S -1) from static pool to each access nodes.

Data prov finds access node such that access node can establish pair wise key with both data req and data prov. If there is direct path establishment then,

Figure 6:- Direct Path

Figure 7:- Indirect Path

In above figure, user select source node as M1 and destination as S2.M1 sends a key to access nodes. Here A3 receives message because A3 found matching key i.e.95608 with M1. A3 also shows available keys of data prov i.e. 582083, 1777467, 1156083.

In direct path panel it shows:

M1:A3 95608 S2 :{ 582083, 1777467}

These shows that M1 and A3 have matching key {95608}.A3 and S2 have matching keys {582083, 1777467}.

If there is indirect path then, find the intermediate data prov node and establish pair wise key with help of intermediate data prov node.

In above figure, user select source node as M1 and destination as S1.M1 sends a key to access nodes. Here A3 receives message because A3 found matching key i.e.95608 with M1. A3 also shows available keys of data prov which is an intermediate node S2 i.e. 582083, 1777467, 1156083.S2 founds matching keys with destination node S1.

In Indirect path panel it shows:

M1:A3 95608 S2 S1 {582083, 1777467}

These shows that M1 and A3 have matching key {95608}.A3 and S2 found same keys which is an intermediate node.S2 and S1 have matching keys {582083, 1777467}.

Figure 8:- Generation of Password Pool

After matching the keys to enhance the security of the network or system password pool is generated.System will ask user to enter the size of the pool and R is randomly generated password where user can manually enter any value for R.

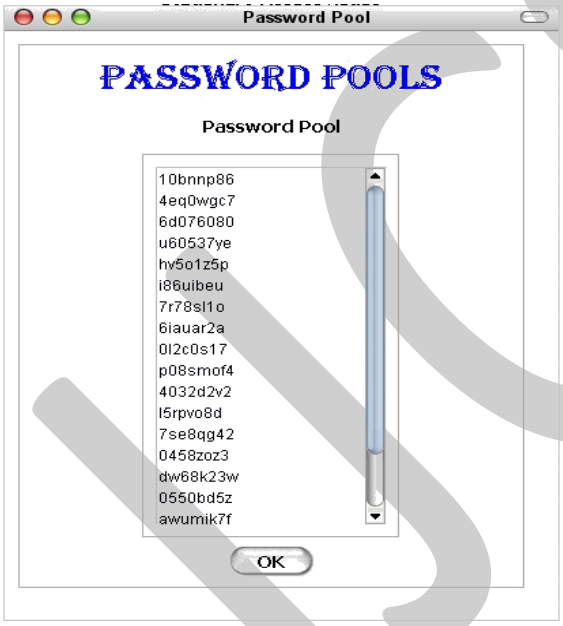

Figure 9:- Password Pool

As shown in above figure passwords are generated.Each password contain combination of digits and alphabets.This password is distributed to only stationary access node and data prov.Stationary access node contain R-1 password from pasword pool and data prov node contain R password from password pool.

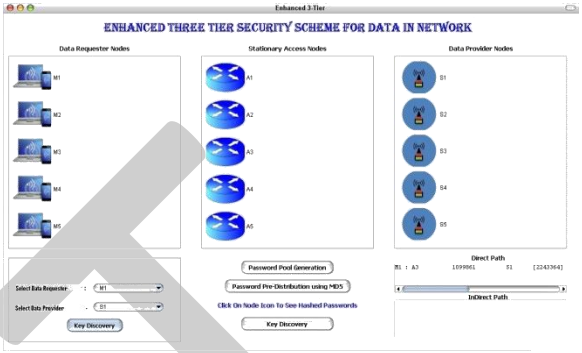

Figure 10:- Password Matching

After the mechanism of matching the keys between data prov and stationary access node, password matching proccess is started between stationary access node and data prov node.Password matching process is running with the keys matching process.

As shown in above figure user will select M1 as source node and S1 as destination node.Password pool is generated and password distribution is done by using MD5(Message Digest).R-1 passwords are assign to access node,R passwords are assign to data prov node from password pool.Path is displayed in the direct path panel which shows direct path establishment between data req and data prov.

Direct path given:

M1:A3 {1099861} S1 { 2243364}

Above path shows that M1,A3 found matching key {1099861} and A3,S1 found matching key {2243364}.In password matching,Rth password from R-1 of

stationary access node gets matched with R password from data prov and more secure path is constructed between data req and data prov.Data is transferred with enhanced or more security.Due to the enhanced security in the system attacker is not able to crack the password provided by the password pool to the stationary access node and data prov node.

VI. CONCLUSION

In this paper, it generation of a three-tier security framework for authentication and pair wise key[4] establishment between data req and data prov. Network security is improved due to data req replication attacks by using polynomial pool based key pre-distribution [3]. Using two separate key pools and having few stationary access nodes our system will not allow an attacker to gather data from data prov by deploying a replicated data req. One-way hash chains algorithm is use for conjunction with the static polynomial pool-based scheme.

VII. REFERENCES

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

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

[3] H. Chan, A. Perrig, and D. Song, "Random Key Pre-Distribution Schemes for Data prov Networks," Proc. IEEE Symp. Research in Security and Privacy, 2003.

[4] D. Liu, P. Ning, and R.Li. Establishing, "Pairwise Keys in Distributed Data prov Networks," Proc. 10th ACM Conf. Computers and Comm. Security (CCS '03), pp. 52-61, Oct. 2003.

[5] A. Rasheed and R. Mahapatra, "A Key Pre-Distribution Scheme for Heterogeneous Data prov Networks," Proc. Int'l Conf. Wireless Comm. and Mobile Computing Conf. (IWCMC '09), pp. 263-268,June 2009.