ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Securing Adhoc Networks Using Group Key Management

D.Rambabu
M.Tech Student
Department of CSE
Raghu Engineering College,
Visakhapatnam.

A.Durga Praveen Kumar, M.S
Assistant Professor
Department of CSE
Raghu Engineering College,
Visakhapatnam.

Abstract:

Security of networks depends on reliable key management systems which generate and distribute symmetrical/asymmetrical (static/dynamic) encryption/decryption keys between communicating parties which will be with the control of one master administrator / super node. This super node will be having following features over the sub nodes.

- *Cast creation: This can create target cast (GROUP) nodes.*
- *Dynamic source node for data transmission.*
- *Encryption and decryption based on algorithm (Rota).*
- *Key generation control algorithm based on SHA-2*

Whenever the transmission is proposed the key will be generated automatically by using SHA-2 for transmission. Here this will be controlled by only super node. Creating the trusted peer as administrator or super peer in wireless adhoc sensor networks is a big challenge. So admin will choose trusted node (in cast of manet) for transmission. Basically nodes can be generated by users request by super node but controlled by on super node. Hence all encryption or decryption and key generation will be at super node level only Traditionally, in wired networks, a central server is responsible to generate and distribute the keys securely. But because of no central server or fixed infrastructure exists in mobile ad hoc networks, there are many difficulties to carryout key management in dynamic and self organized mobile ad hoc networks. The dynamic change in topology results in the change of trust relationship among the nodes. In this paper, we have proposed a key management scheme in grouped network structure in which group leader of a group is randomly shifted, our scheme of key management doesn't require any trusted third party. The group leader is responsible to generate and distribute ids and public-private key pair to nodes. This method reduces the quantity of keys to distribute among the nodes.. Basically the user can create source and destinations (casting nodes) for encrypted (all possible selected formats) for data transmission. The encryption and decryption is user's choice (according to mode of transmission).

Index Terms: *Cast, Group, Peer, Peer Level, Secure communication, SNMP, SMTP*

1. Introduction:

Securing a computer network requires mastery of many skills and concepts are proper design of network, device and deployment, protocols, etc.

Existing concerns in network security:

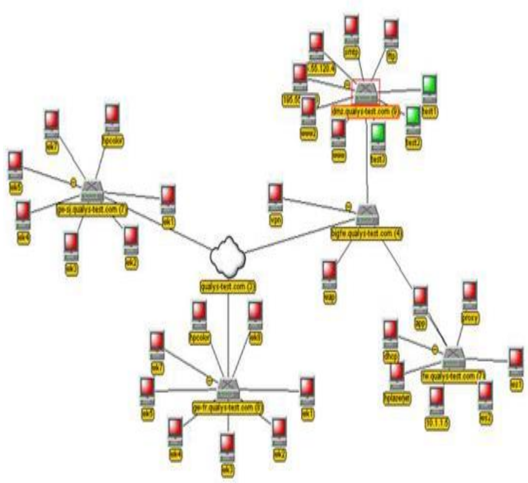
- The issues can arise if there are IP based phones on a network that uses the same port!
- It will be possible to get the following data from IDS.

- Total number of packets that node receives from one single destination only.
- Total number of packets that node receives from all sources.
- The time between two received packets.
- Wheatear to check the information from a security aspect, or the focus is towards other data nodes
- If public SMTP servers are located in a perimeter network, what is the procedure for tunneling internal mail through the firewall?
- Under what parameters or boundaries would you recommend building your own intrusion detection system (IDS)?
- Which way the client will connect/reconnect without using secure socket layers able to connect to remote secure server?

To overcome above concerns this paper proposed this DYN Peer proposal algorithm to have tree structure adhoc network (can be migrated to other topology with in no time of migrating to other networks instantly. DYN Peer proposal generates prior static peer adhoc network and after that it will instantly acts as dynamic peer addition/deletion at any instant of working network. This Three level key protection is available in this algorithm for secure packet TCP/IP transmission over the tree adhoc network.

The main purpose of DYN Peer proposal to overcome the instant casting issues as target nodes. The source node is always can be any one in available adhoc network and casing nodes(group nodes as target nodes) to transmit data and both will be controlled by administrator peer which is ROOT node in tree network. The node which is sending the data will be protected by keys to transmit the data. The following are the available keys in our proposal.

Architecture Diagram:



Existing System:

- The issues can arise if there are IP based phones on a network that uses the same port.
- It will be possible to get the following data from IDS.
- If public SMTP servers are located in a perimeter network.
- Whether to check the information from a security aspect, or the focus is towards other data nodes.

Disadvantages:

One of the drawbacks with SHA-2 is that there are some older applications and operating systems that do not support it. Compatibility problems are the main reason why SHA-2 algorithms have not been adopted more rapidly. Windows XP Service Pack 2 or lower does not support the use of SHA-2. The use of SHA-2 on websites may pose a problem if the end user has an older operating system.

Regarding server side support for SHA-2, there are a few things that need to be considered. If you are using a Windows environment, Microsoft has published the following blog for SHA-2 deployment. You will need to make sure you have the minimum supported version of Windows server, along with any required patches that are mentioned.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Proposed System:

We propose SHA 3 Algorithm to overcome the problem of SHA -3 (SANUGKM) is to create the static/dynamic peers (in simulated adhoc network), which will be with the control of one master administrator / super node.DYN Peer proposal algorithm to have tree structure adhocnetwork (can be migrated to other topology with in no time of i.e. migrating to other networks instantly. DYN Peer proposal generates prior static peer adhoc network and after that it will instantly acts as dynamic peer addition/deletion at any instant of working network. This Three level key protection is available in this algorithm for secure packet TCP/IP transmission over the tree adhoc network.

Advantages:

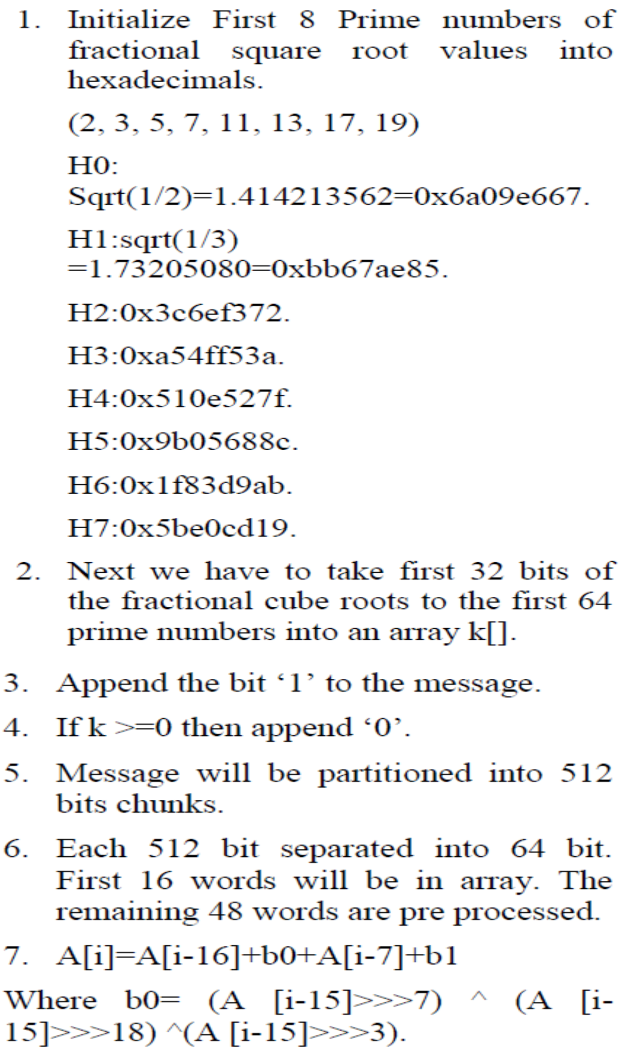
- Rota encryption provides high security for data files while transmitting data from node to node in manet.
- SHA-3: A hash function formerly called Keccak, chosen in 2012 after a public competition among non-NSA designers. It supports the same hash lengths as SHA-2, and its internal structure differs significantly from the rest of the SHA family.
- The corresponding standards are FIPS PUB 180 (original SHA), FIPS PUB 180-1 (SHA-1), FIPS PUB 180-2 (SHA-1, SHA-256, SHA-384, and SHA-512). NIST has updated Draft FIPS Publication 202, SHA-3 Standard separate from the Secure Hash Standard (SHS).
- The main advantage of sha-2 algorithm is it generates same size of key for any size of plain text. so we can specify the size for key.
- In SNMP multiple peers can be managed but very few adhoc networks have the following features: (Dynamic peer generation with static peer network, data sharing among unlimited casting peers as destination group, SHA-2 for secure key generation).
- Logs will be maintained instantly with micro level information.

Implementation Modules:

1. Administration peer in wireless Adhoc sensor network (Math part)
2. Group/key Management
   - Adding key
   - Deleting key
   - Rekeying/refreshing key
3. Data Transmission/tracking management using algorithm(s).

Metrics table (bw,size,time)

SHA-2 Algorithm:



1. Initialize First 8 Prime numbers of fractional square root values into hexadecimals.

   (2, 3, 5, 7, 11, 13, 17, 19)

   H0: Sqrt(1/2)=1.414213562=0x6a09e667.

   H1:sqrt(1/3) =1.73205080=0xbb67ae85.

   H2:0x3c6ef372.

   H3:0xa54ff53a.

   H4:0x510e527f.

   H5:0x9b05688c.

   H6:0x1f83d9ab.

   H7:0x5be0cd19.

2. Next we have to take first 32 bits of the fractional cube roots to the first 64 prime numbers into an array k[].

3. Append the bit '1' to the message.

4. If k >=0 then append '0'.

5. Message will be partitioned into 512 bits chunks.

6. Each 512 bit separated into 64 bit. First 16 words will be in array. The remaining 48 words are pre processed.

7. A[i]=A[i-16]+b0+A[i-7]+b1

Where b0= (A [i-15]>>>7) ^ (A [i-15]>>>18) ^(A [i-15]>>>3).

```
    b1= (A [i-2]>>>17) ^ (A [i-2]>>>19) ^(A [i-2]>>>10).
8.  a←H0,b←H1,c←H2,d←H3,e←h4,f←H5,g←H6,h←H7
9.  Loop starts I =0-63
        B1= (e>>>6) ^ (e>>>11) ^ (e>>>24)
        Ch= (e ∧ f) ^ (⌐ e ∧ g)
        Temp1=h+b1+ch+k[i] +A[i]
        B0= (e>>>2) ^(e>>>13) ^(e>>>22)
        Maj=(a∧b)^(a∧c)^(b∧c)
        Temp2=b0+maj;
10. Replace values as while appending
        h=g
        g=f
        f=e
        e=d+temp1;
        d=c
        c=b
        b=a
        a=temp1+temp2;
```

Rota Encrypt/Decrypt Algorithm:

Encryption:

Input: Plain text

Output: CipherText

```
Initialization:
n←0 //total number of characters.
∑D←0 //total data
Cipher←1
∑E←0            //total Encrypted data
t1←null         //temp variable
t2←null         //temp variable
Loop for each c in D
        n=0
        t1←LSHIFT(c,n,CIPHER)
        t2←RSHIFT(c,n+1,CIPHER)
                n+1
        E←APPEND(t1)
        E←APPEND(t2-1)
End loop
```

Decryption:

Input: Cipher text

Output: Plain text

```
Initialization:
N←0 //initialization for total number of characters.
∑E←0 //Cipher texts
∑N←0        // plain text
T1←null
T2←null
Loop for each c in E
n=0
t1←RSHIFT(c,n,CIPHER)
t2←LSHIFT(c,n+1,CIPHER)
            n+1
      D←APPEND(t1)
      D←APPEND(t2+1)
End loop
```

CONCLUSION

Secure Group Management would explain us to maintain the security relations between peer in manet. Here we can permit the nodes by providing the Root key for adding node and for removing nodes. The region of wireless nodes is communicated by transmitting the data with encryption format by using the advanced Algorithms what we had implemented in this paper. While implementation we got best results and performance.

References:

[1] A. Perrig, "Efficient Collaborative Key Management Protocols for Secure Autonomous Group Communication", 1999.

[2] T. Dunigan and C. Cao, "Group Key Management", 1998.

[3] A. Ballardie, "Scalable Multicast Key Distribution", 1996.

[4] R. Canetti and B. Pinkas, "A Taxonomy of Multicast Security Issues", 1998.

[5] M. Waldvogel, G. Caronni, D. Sun, N. Weiler and B. Plattner, "The VersaKey Framework: Versatile Group Key Management", 1999.

[6] G. Caronni, M. Waldvogel, D. Sun and B. Plattner, "Efficient Security for Large and Dynamic Multicast Groups", 1998.

[7] I. Chang, R. Engel, D. Kandlur, D. Pendarakis and D. Saha, "Key Management for Secure Internet Multicast using Boolean Function Minimization Techniques", 1999.

[8] T. Hardjono, M. Baugher and H. Harney, "Group Security Association (GSA) Management in IP Multicast", 2000.

[9] O. Rodeh, K. Birman and D. Dolev, "Using AVL Trees for Fault Tolerant Group Key Management", 2000.

[10] B. Bhargava, S. B. Kamisetty and S. K. Madria, "Fault-tolerant Authentication and Group Key Management in Mobile Computing", 2000.

[11] P-C Cheng, J. A. Garay, A. Herzberg and H. Krawczyk, "Design and Implementation of Modular Key Management Protocol and IP Secure Tunnel on AIX", 1995.