ISSN:0975-9646

A Novel Secured Protocol for Data Transmission in Adhoc Networks Using Clustering

K.Komali
M.Tech Student,
Dept of cse,AIET

V.Mahesh
Asst. Professor,
Dept of CSE, AIET

Y.Ramesh Kumar
Asst. Professor,
Dept of CSE, AIET

Abstract:we propose a secure communication protocol for communication between two nodes in ad hoc networks. This is achieved by using clustering techniques. We present a novel secure communication framework for ad hoc networks (SCP); which describes authentication and confidentiality when packets are distributed between hosts with in the cluster and between the clusters. These cluster head nodes execute administrative functions and network key used for certification. The cluster head nodes (CHs) perform the major operations to achieve our SCP framework with help of RSA and DH AlgorithmsA network is divided into clusterswith one special head node each. These cluster head nodes executeadministrative functions and hold shares of a network key usedfor certification. New nodes start to participate in the networkas guests; they can only become full members with a network signed certificate after their authenticity has been warranted bysome other members. The feasibility of this concept was verified by simulation. Three different models for node mobility wereused in order to include realistic scenarios as well as make theresults comparable to other work. The simulation results includean evaluation of the log-on times, availability, and communicationoverhead.

Keywords: adhoc-networks, cluster, cluster-head, encryption, decryption, cryptography.

1. INTRODUCTION

Ad hoc network is a collection of nodes that do not need to rely on a predefined infrastructure to keep the network connected. *Availability* ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network.

Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality.

Integrity guarantees that a message being transferred is never corrupted or altered.

Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation and other nodes.

Non-repudiation ensures that the origin of a message cannot deny having sent the message; non-repudiation is useful for detection and isolation of compromised nodes.

Adhoc network applications

Military Battlefield ad hoc networking would allow the military to take advantage of common place network technology to maintain an information network between the soldiers, vehicles, and military information head quarters. The basic techniques of ad hoc network came from this field.

Commercial Sector ad hoc network can be used in emergency or rescue operation for disaster relief efforts e.g. in fire, flood, and earthquake etc. Other commercial scenarios include e.g. ship-to-ship ad hoc mobile communication, law enforcement, etc.

Local Level ad hoc networks can autonomously link an instant and temporary multimedia network using notebook computers or palmtop computers to spread and share information among participants at a e.g. conference or classroom. Similarly in other civilian environments like taxicab, sports stadium, boat and small aircraft, etc.

Personal Area Network (PAN) intercommunication between various mobile devices such as PDA, laptop, cellular phone, etc.

Adhoc network major challenges

Routing since the topology of the network is constantly changing; the issue of routing packets between any pair of nodes becomes a challenging task. Most protocols should be based on reactive routing instead of proactive. Multicast routing is another challenge because the multicast tree is no longer static due to the random movement of nodes. Routes between nodes may potentially contain multiple hops, which is more complex than the single hop communication.

Security and Reliability some common vulnerability of ad hoc wireless connections is Sinkhole attack, Sybil attacks, and Acknowledge Spoofing,

Quality of Service providing different quality of service level in a constantly changing environment will be a challenge.

Internetworking between mobile ad hoc networks and fixed networks is often expected in many cases, which leads to a challenging task.

Power Consumption for most of the light weight mobile terminals, the communication related functions should be optimized for lean power consumption. Conservation of power and power-aware routing must be taken into consideration.

Existing Scheme Analysis shows the techniques which have been proposed already, here we going to see the merits and demerits of the existing technique which leads to proposal of our scheme.

Threshold cryptography is one of the secret sharing techniques. A trusted dealer divides a secret D into n parts so that the knowledge of k parts ($k \leq n$) allows the reconstruction of the secret, which is not possible with the knowledge of k-1 or fewer parts.

In proactive secret sharing scheme, secret shares are changed periodically without changing the secret itself, so an attacker cannot use a secret whole lifetime to compromise k participants. All information an attacker collected about the secret becomes worthless after refreshing the shares.

The key distribution center (KDC), the central entity is responsible for the key management in a secret key infrastructure. In this, a group of servers jointly act as a KDC with each server sharing a unique secret key with each client.

General Model of SCP

Communication with adjacent clusters. The GWs may or may not be CHs. The CHs are responsible for sending CH beacons in their clusters, containing administrative information for the cluster members, e.g., lists of nodes and GWs in the cluster. Also, GWs periodically transmit GW beacons to inform their respective clusters about adjacent clusters. Clustering is also used in some routing protocols for ad hoc networks. Routing is then typically divided into two parts: routing within a cluster (intra-cluster) and routing between different clusters (inter-cluster). One solution for such a scenario is the zone routing protocol, a combination of proactive intra-cluster and reactive inter-cluster routing; communication between two clusters is always routed via GWs.

In our approach, two keys are used one key used for communication between cluster heads and gateway, another key is used by the nodes in the clusters. When a cluster head moves or become unreachable, the high priority node in the cluster becomes the cluster head. The new CH gets the shared key of old CH from the neighboring CH. Also we need to make sure that the key needs to be renewed or changed after a certain period of time in order to make it hard for a moving attacker to compromise a number of k CHs over time.

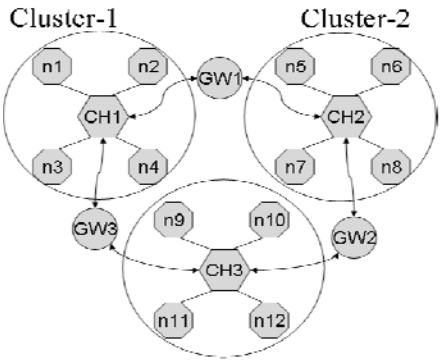

Fig.1. General Model of SCP

Format of information stored in CH database are as follows

CHid	Nid	Pn	NAn

The same above format is used by GW but it will not store information about password (Pn).

Log on process *for a new node* When new node receives the beacon signal from a cluster, if it want to join in that cluster it send its information, which consists of network address Nan and public key of the new node Kun and the message is encrypted by using public key of corresponding cluster head. The CH receives the message and decrypts it using its private key and checks the information is correct. If they are correct CH generates node id Nid and secret master key Knch which is known to new node and CH. The message is encrypted using public key of new node and sends it to new node. The new node decrypts the message and store the node id and master key. Further communications between nodes are established by using the master key.

1) N → CH **:** Ekuch [Nan || Kun]
2) CH → N **:** EKun [Nid || Knch]

NAn → Network Address of a node.
Nid → Node Identifier.
Kuch → Public key of CH
Kun → Public key of ode N.

*Secure Communication between two nodes within cluster*When two nodes want to communicate, consider for example N1 wants

Classification of Algorithms

RSA Algorithm

In cryptography, RSA is an algorithm for public-key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations. The algorithm was described by Ron Rivest, Adi Shamir and Leonard Adleman at MIT; the letters are the initials of their surnames. RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with

The public key can only be decrypted using the private key. The keys for the RSA algorithm are generated the following way:

Choose two distinct large random prime numbers p and q.

Compute $n = pq$, n is used as the modulus for both the public and private keys

Compute the Quotient: $\phi(n) = (p-1)(q-1)$.

Choose an integer e such that 1 <e<φ(n), and e and φ(n) share no factors other than 1 (i.e. e and φ(n) are co prime) .

e is released as the public key exponent.

Compute d to satisfy the congruence relation

$de \equiv 1 \pmod{\phi(n)}$;

i.e.

de = 1 + kφ (n) for some integer k.

d is kept as the private key exponent.

To encrypt a message M:

The sender obtains public key of recipient KU={e,N}

Computes: $C=M^e \bmod N$, where $0 \le M < N$

To decrypt the ciphertext C:

The owner uses their private key KR={d,N}

Computes: $M=C^d \bmod N$

Diffie-Hellman key exchange

Diffie-Hellman key exchange (**D-H**) is a cryptographic protocol that allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure communications channel. This key can then be used to encrypt subsequent communications using a symmetric key cipher.

History of the protocol

Diffie-Hellman key agreement was invented in 1976 during collaboration between Whitfield Diffie and Martin Hellman and was the first practical method for establishing a shared secret over an unprotected communications channel. The method was followed shortly afterwards by RSA, another implementation of public key cryptography using asymmetric algorithms

Description

Diffie-Hellman key exchange

The simplest, and original, implementation of the protocol uses the Multiplicative group of integer's module p, where p is prime and g is primitive root mod p. Here is an example of the protocol:

1. Alice and Bob agree to use a prime number p=23 and base g=5.
2. Alice chooses a secret integer a=6, then sends Bob A=(g^a mod p) A = 5^6 mod 23 = 8.
3. Bob chooses a secret integer b=15, then sends Alice B=(g^b mod p) B = 5^{15} mod 23 = 19.
4. Alice computes s = $(B)^a$ mod p

19^6 mod 23 = 2.

5.Bob computes s = $(A)^b$ mod p

8^{15} mod 23 = 2.

Here's a more general description of the protocol:

1. Alice and Bob agree on a finite cyclic group G and a generating element g in G. (This is usually done long before the rest of the protocol; g is assumed to be known by all attackers.) We will write the group G multiplicatively.
2. Alice picks a random natural number a and sends g^a to Bob.
3. Bob picks a random natural number b and sends g^b to Alice.
4. Alice computes $(g^b)^a$.
5. Bob computes $(g^a)^b$.

Both Alice and Bob are now in possession of the group element g^{ab}, which can serve as the shared secret key. The values of $(g^b)^a$ and $(g^a)^b$ are the same because groups are power associative.

Security

The protocol is considered secure against eavesdroppers if G and g are chosen properly. The eavesdropper ("Eve") would have to solve the Diffie-Hellman problem to obtain g^{ab}. This is currently considered difficult. An efficient algorithm to solve the discrete logarithm problem would make it easy to compute a or$b$ and solve the Diffie-Hellman problem, making this and many other public key cryptosystems insecure.

The order of G should be prime or have a large prime factor to prevent use of the Pohlig-Hellman algorithm to obtain a or$b$. For this reason, a sophieger main prime q is sometimes used to calculate $p=2q+1$, called a safe prime, since the order of G is then only divisible by 2 and q. $g$is then sometimes chosen to generate the order q subgroup of G, rather than G, so that the Legender symbol of g^a never reveals the low order bit of a.

If Alice and Bob use random number generators whose outputs are not completely random and can be predicted to some extent, then Eve's task is much easier.

The secret integers a and$b$ are discarded at the end of the session. Therefore, Diffie-Hellman key exchange by itself trivially achieves perfect forward secrecy because no long-term private keying material exists to be disclosed.

Authentication

In the original description, the Diffie-Hellman exchange by itself does not provide authentication of the communicating parties and is thus vulnerable to a man-in–middle attack. A person in the middle may establish two distinct Diffie-Hellman key exchanges, one with Alice and the other with Bob, effectively masquerading as Alice to Bob, and vice versa, allowing the attacker to decrypt (and read or store) then re-encrypt the messages passed between them. A method to authenticate the communicating parties to each other is generally needed to prevent this type of attack.

2. METHODOLOGY

Kerberos provides a centralized authentication server whose function is to authenticate user to server and server to user. Kerberos relies exclusively on symmetric encryption. In ad hoc network central entity is easy to attack. In our architecture we using clustering technique, where each cluster has is own cluster head (CH) nodes. These CH act as a Kerberos server for a set of nodes. Due to periodic change of CH in a cluster we can prevent the networks from attack. By using Kerberos authentication application we can achieve Secure, Reliable, Transparent, Scalable, and less overhead.

Assumptions In our proposed scheme we have made the following assumptions:

1. All CH and GW share a key with each other.
2. All CH and GW are honest nodes.
3. The CH and GW are static nodes.

In order to make our concept scalable, to avoid expensive long-range traffic, and to enhance availability by providing service locally, we partition an ad hoc network into a number of clusters. In each cluster, exactly one distinguished node – the cluster head (CH) – is responsible for establishing and organizing the cluster. Gateways (GW), manage

When a new node enters into a particular cluster, the CHs generate identification number (ID) and password. This ID and password are used when two nodes communicates. The communication takes place via CHs; CHs use the node ID and password to check the authenticity of the particular node which requests. CHs maintain a table of information about the nodes in the network. When new node enters in one cluster it stores necessary information in the CHs and alsointimate to other clusters. By using the ID and network address of the node we can say that the message comes from a authenticated node. By using the symmetric key encryption we can say that message is not altered and provide confidentiality. Thus by using our proposed scheme we can achieve authentication and confidentiality for the communication between nodes.

Advantage of using symmetric key cryptographic technique:

- Scalable since we are dividing network into cluster.
- Less overhead.
- Reliable.

. Only n keys are used not n*(n-1).

Advantage of using Kerberos Authentication Application:

. Single server needs to be accessed

. Faster authentication

. Reduced client side processing.

Advantage of using Clustering Technique:

. Spatial reuse of resources, which can significantly improve the system capacity.

. Reduce the amount of routing information in the network.

. Reduce the amount of routing delay in the network.

Known to N1 and CH only. CH decrypts the message and check whether the destination N2 is with in the cluster. If so CH generates a packet which consists of session key Ks, N1id, N2id and Ekn2ch [ks || N1id]. The packet is encrypted by using the master key and sends it to N1. N1 decrypts the packet and send N1id and Ekn2ch [ks || N1id] to the destination node N2. N2 decrypts the packet and compare the encrypted N1id with unencrypted N1id if they are correct N2 identifies that N1 is an authenticated node and sends acknowledgement to N1. Then further communication is established using the session key. the Operation of communication between two nodes with in cluster is

1) N1 → CH : Ekn1ch [N1id || N2id]
2) CH → N1 :Ekn1ch [Ks || N1id || N2id || Ekn2ch [ks || N1id]]
3) N1 → N2 : N1id || Ekn2ch [ks || N1id]
N1, N2 → Nodes
N1id → Identifier of node N1
N2id → Identifier of node N2
CH → Cluster Head
Kn1ch → Secret Key Known to CH and N1.
Kn2ch → Secret Key Known to CH and N2.
Ks → Session Key
5) CH2→CH1 :Ekch [Ks || N1id || N2id || Ekn2ch2 [Ks||N1id]]
6) CH1→N1 : Ekn1ch1 [Ks || N1id || N2id || Ekn2ch2 [Ks||N1id]]
7) N1 → N2 : N1id || Ekn2ch2 [Ks || N1id]
N1, N2 → Nodes
N1id, N2id → Identifier of node N1 and N2
CH1, CH2 → Cluster Heads
CH1id → Identifier of CH1.
CH2id → Identifier of CH2.
Kch → Key known to CH and GW

Basic operation is as shown in below figure

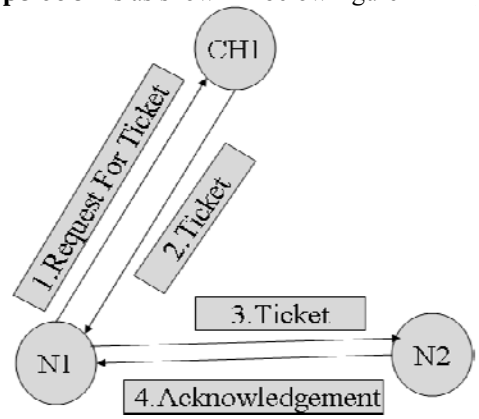

Figure2:basic operation.

4. ADVANCED ENCRYPTION STANDARD ALGORITHM (AES):

The Advanced Encryption Standard (AES) is a specification for the encryption of electronic data established by the U.S.National Institute of Standards and Technology (NIST) in 2001[8]

AES is a block cipher, but it does not use a Feistel structure. The block size of AES is 128-bit, but the key size may differ as 128, 192, or 256 bits [9].

Substitution: This method substitutes each byte of the block in the order of S-box. It provides an invertible transformation of blocks during encryption, with the reverse during decryption.

Shifting Rows: This operation performs left circular shifts of rows 1, 2, and 3 by 1, 2 and 3,

Mix Columns: This method multiplies each column of the input block with a matrix. The multiplication operation is just like matrix multiplication, except that it uses a Finite Field to multiply two elements and performs an XOR operation instead of addition.

Add Rounded Keys: This operation just applies an XOR operation to each byte of the input block and the current weight (key) matrix.

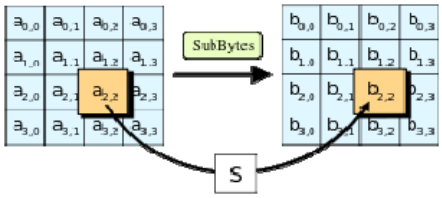

Figure 3:the Sub-Bytes step, one of four stages in a round of AES

4. DATA ANALYSIS

Node selection as shown in below figure:

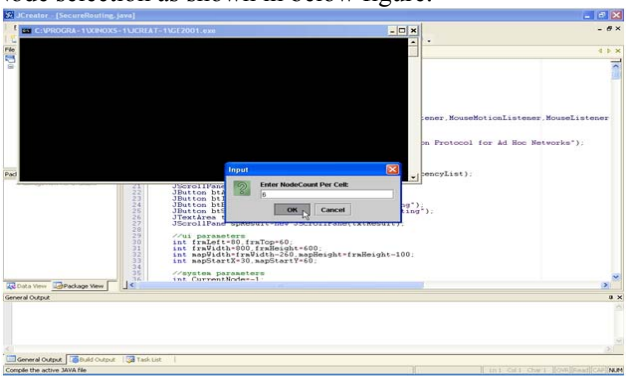

Figure 4
Selection of Authentication

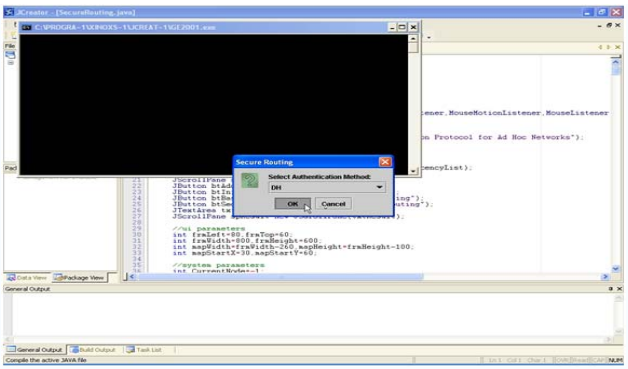

Figure 5
Cluster as shown in below figure5

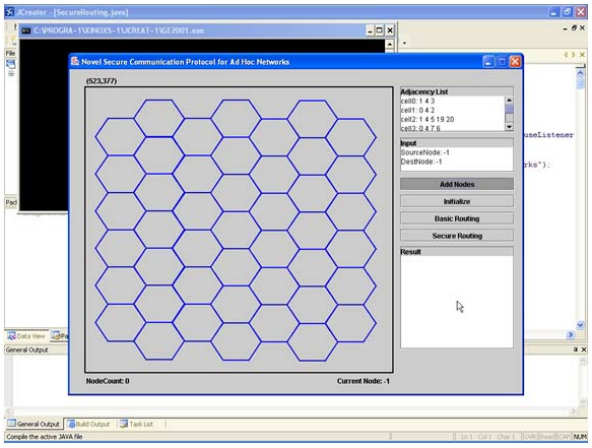

Figure 6

Every cluster contains cluster head and nodesas shown in figure 6

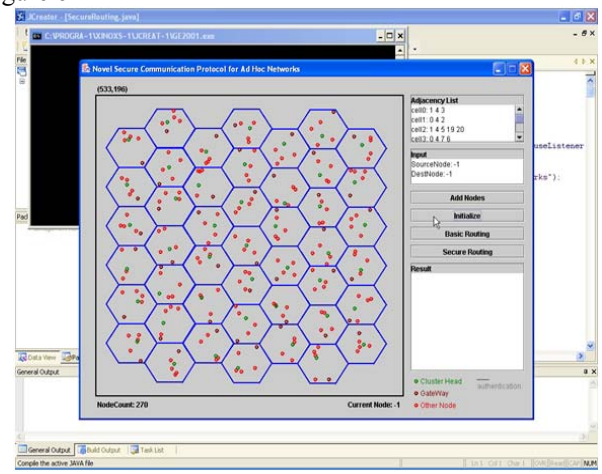

Figure 7

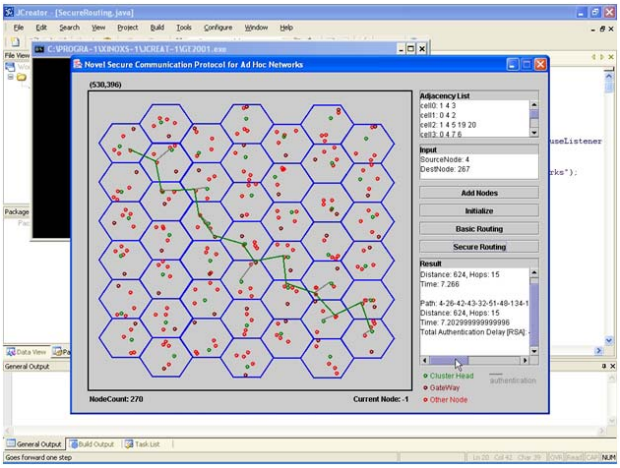

Figure 8

Path beteen one nodfe in one cluster to another node another cluster is shown in figure 7,8

CONCLUSION

In this paper, we introduced a cluster based secure authentication protocol framework for symmetric key infrastructure, based on the clustering technique and Kerberos authentication application for an ad hoc network. Also we have analyzed the security issues, challenges, goals, application and analysis of existing scheme of an ad hoc network and presented the security objective that needs to be achieved.

Our future work includes doing further explorations to evaluate our architecture through security analysis andsimulations.

REFERENCES

1. M. Bechler, H.-J. Hof, D. Kraft, F. Pählke, L. Wolf, “A Cluster-Based Security Architecture for Ad Hoc Networks”, IEEE Infocom 2004.
2. L. Zhou and Z.J. Haas, “ Securing Ad Hoc Networks”, IEEE Network, Vol.13, no.6, pp.24-30, 1999.
3. V. Kärpijoki, “Security in Ad Hoc Networks”, Helsinki University of Technology, Telecommunications Software and Multimedia Laboratory.
4. A.Perrig, R.Canetti, J.D.Tygar, D.Sang, “The TESLA Broadcast Authentication Protocol”, IN CryptoBytes, 5:2, summer/fall 2002, pp.2-13.
5. K. Inkinen, “New Secure Routing in Ad Hoc Networks: Study and Evaluation of Proposed Schemes”, Helsinki University of Technology, Laboratory of Multimedia.
6. H. Lue, P. Zerfos, J. Kong, S. Lu and L. Zhang, “Self- Securing Ad Hoc Wireless Networks”, IEEE ISCC 2002.
7. D. Balfanz, D.K. Smetters, P. Stewart and H. Chiwong, “Talking To Strangers: Authentication in Ad Hoc Wireless Networks”, Internet Society, Xerox Palo Alto Research Center.
8. K.Fokine, “Key Management in Ad Hoc Networks”, LITH-ISY-EX-3322-2002 2002-09-11.
9. A. Shamir, “How to Share a Secret”, Acm Comm., Vol.22, no.11, 1979.
10. A. Herzberg, M. akobson, S. Jarecki, H. Krawczyk, and M. Yung, “Proactive Public Key and Signature Systems”, in AcmConf, on Computer and Comm. Security, ziirich, 1997.
11. C. Perkins, “Ad Hoc Networking”, Addison-Wesley, 2001.
12. W. Stallings, “Cryptography and Network Security: Principle and Practice”, Third Edition, Prentice-Hall 2003.
13. Jon-Zhao Sun,” Mobile Ad Hoc Networking: An Essential Technology for Pervasive Computing”, University of Oulu, Finland.