Global Journal of Computer Science and Technology
Volume 11 Issue 13 Version 1.0 August 2011
Type: Double Blind Peer Reviewed International Research Journal
Publisher: Global Journals Inc. (USA)
Online ISSN: 0975-4172 & Print ISSN: 0975-4350

Key Protocol Coordination in Mobile Ad-Hoc Networks

By Mr.N.Satish Kumar, Dr.N.Satyanarayana

Nagole Institute of Technology & Sciences Hyderabad.A.P. INDIA

Abstract - In this paper we propose and design key authentication protocols for wireless networks. We consider three mobile service domains; each has an authentication server. We denote by D1, D2 and D3 corresponding authentication servers. For simplicity, let D1, D2 ,D3 represent those three domains. This mobile system can provide mobile communication services to a large number of users. For simplicity, we assume three users (A, B and C) in the system only, where A has registered with D1 and B has registered with D2 and C has registered with D3.

GJCST Classification : *C.2.1, C.2.2*

Strictly as per the compliance and regulations of:

Key Protocol Coordination in Mobile Ad-Hoc Networks

Mr.N.Satish Kumar[α], Dr.N.Satyanarayana[Ω]

Abstract : In this paper we propose and design key authentication protocols for wireless networks. We consider three mobile service domains; each has an authentication server. We denote by D1, D2 and D3 corresponding authentication servers. For simplicity, let D1, D2 ,D3 represent those three domains. This mobile system can provide mobile communication services to a large number of users. For simplicity, we assume three users (A, B and C) in the system only, where A has registered with D1 and B has registered with D2 and C has registered with D3.

I. Introduction

a) Symmetric-key

An encryption system in which the sender and receiver of a message share a single, common key that is used to encrypt and decrypt the message. Contrast this with public-key cryptology, which utilizes two keys - a public key to encrypt messages and a private key to decrypt them. Symmetric-key systems are simpler and faster, but their main drawback is that the two parties must somehow exchange the key in a secure way. Public-key encryption avoids this problem because the public key can be distributed in a non-secure way, and the private key is never transmitted. Symmetric-key cryptography is sometimes called *SECRET-KEY CRYPTOGRAPHY.* The most popular symmetric-key system is the *DATA ENCRYPTION STANDARD.*

b) Types

Symmetric- key algorithms can be divided into stream ciphers and block ciphers. Stream ciphers encrypt the bits of the message one at a time, and block ciphers take a number of bits and encrypt them as a single unit. Blocks of 64 bits have been commonly used. The Advanced Encryption Standard (AES) algorithm is approved by NIST where uses 128-bit blocks. Examples of some symmetric algorithms include Twofish, Serpent, AES (Rijndael), Blowfish, CAST5, RC4, TDES, and IDEA.

c) Security issue

Symmetric ciphers have historically been susceptible to known-plaintext attacks, chosen plaintext attacks, differential cryptanalysis and linear crypt-analysis. Careful construction of the functions for each round can greatly reduce the chances of a successful attack.

Author[α]: Associate Professor, Department of CSE, School of Engineering, SVS Group of Institutions, Bheemaram,Warangal-506 013,A.P. INDIA . E-mail : satish4info@gmail.com
Author[Ω] : Professor, Department of CSE, Nagole Institute of Technology & Sciences Hyderabad.A.P. INDIA .
E-mail : nsn1208@gmail.com

d) Inter Domain

In computing, **inter-domain** is a term used to describe interaction between domains. It is most commonly used in the fields of multicasting and routing between internets, or as a substitute for the term inter-server. Internet protocols that are focused on inter-domain functions include: Border Gateway Multicast Protocol, Classless Inter-Domain Routing, Multicast Source Discovery Protocol, and Protocol Independent Multicast. The opposite of inter-domain routing is intra-domain routing (routing within a domain or an autonomous system).

e) End-To-End Authentication

An authentication protocol is a type of cryptographic protocol with the purpose of authenticating entities wishing to communicate securely. There are many different authentication protocols such as: Kerberos, RADIUS (Remote Authentication Dial In User Service) and so on. End to end authentication protocol is a computer network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. It provides mutual authentication — both the user and the server verify each other's identity.

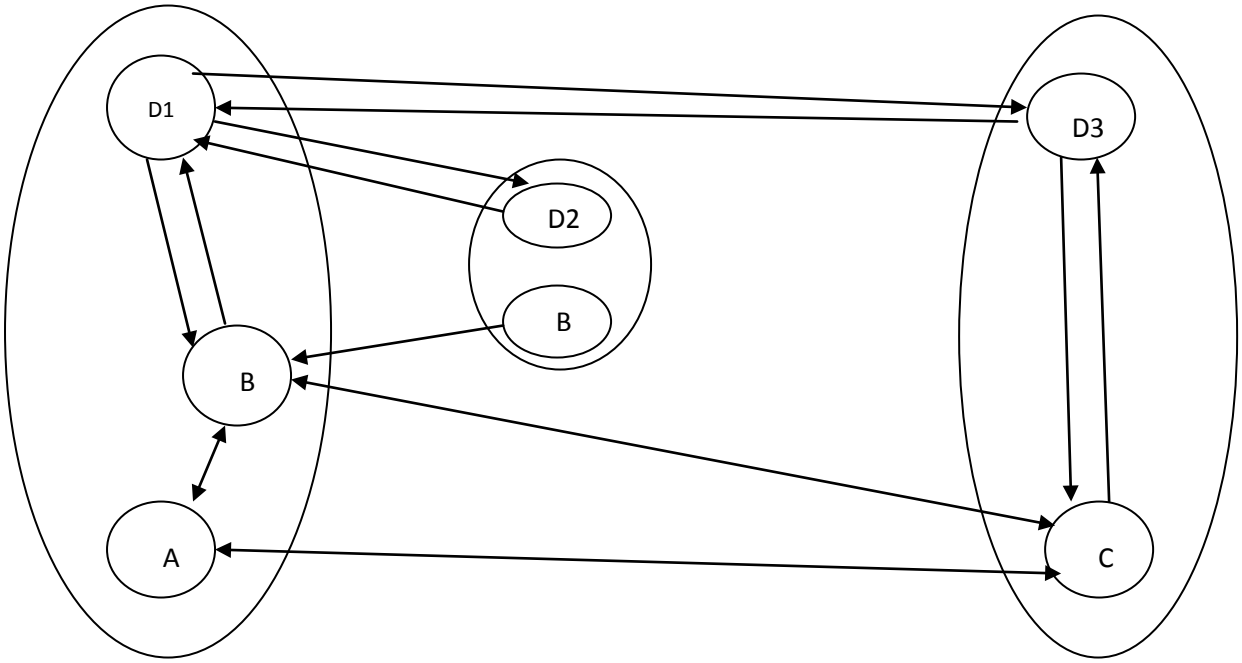
II. Proposed Protocol Design

a) Notations

D1 – Domain Server of user A and foreign domain server for B and C
D2 – Domain Server of user B and foreign domain server for A and C
D3 – Domain Server of user C and foreign domain server for A and B

A –> B: *message:* This means A sends message to B.
A –> C: *message:* This means A sends message to C.
B –> A: *message:* This means B sends message to A.
B –> C: *message:* This means B sends message to C.
C –> B: *message:* This means C sends message to B.
C –> A: *message:* This means C sends message to A.
B_s –> Identity of B

b) Protocol Illustration & Descriptions



STEP 1 : B → D1

- B sends D1 a request, including a Token, nonce, "identity package" and hash value. B's subliminal identity for anonymity.
- The Token is encrypted so as to be passed on to D2 without D1 being able to read it.
- The content of the Token will allow D2 to authenticate B.
- D1 cannot verify the hash value or decrypt the request, since it doesn't have $K_{B,D1}$, which is generated using a strong one-way hash function f.

STEP 2 : D1 → D2

- After receiving the Token, the Home server D2 is able to authenticate B.

STEP 3 : D2 → D1

- D2 sends a new identity.
- The identity and second hash value will be passed to B
- D2 gives the key $K_{B,D1}$ and B's identity.
- D1 can use this to verify the hash value received from B_S in the first step.
- D1 now knows who B_S wants to talk.

STEP 4 : D1 → D3

- Verification of the request, D1 generates a secret session key K_S, which is for distribution to A and C.
- D1 passes the identity to D2, otherwise C at far end won't be satisfied that A and B are trying to communicate with them later.

STEP 5 : D3 → C

- D3 passes the secret session key K_S, along with A's, B's and C's identities and the nonce n_B, along to C encrypted under $K_{D3,B}$.
- Authentication of B to C is complete.
- D3 also send an updated identity(for C)at this stage.

STEP 6 : C → D3

- Start authentication of C to B. C sends D3 the hash value containing the secret session key K_S, and A's, B's and C's identities

STEP 7 : D3 → D1

- Upon verification of the hash value, D1 is aware of whether or not C has received the correct session key, and whether the information is fresh.
- The identity of C is being passed back for B and A to use.

STEP 8 : D1 → B

- D1 sends everything it can find
- It distributes the session key K_S
- B receives its new identity for use in the future communications.
- D1 also send A's new identity.

STEP 9 : B → A

- B distributes the session key K_S, encrypted under $K_{A,D1}$ for A.
- A receives its new identity for use in the future communication.

STEP 10 : A → B

- A sends message to B with nonce and under encrypted with session key K_S.

STEP 11 : B → C

- B sends message to C with nonce and under encrypted with session key K_S.

STEP 12 : C → B

- C sends message to B with nonce and under encrypted with session key K_S.

STEP 13 : A → C

- A sends message to C with nonce and under encrypted with session key K_S.

STEP 14 : C → A

- C sends message to A with nonce and under encrypted with session key K_S.

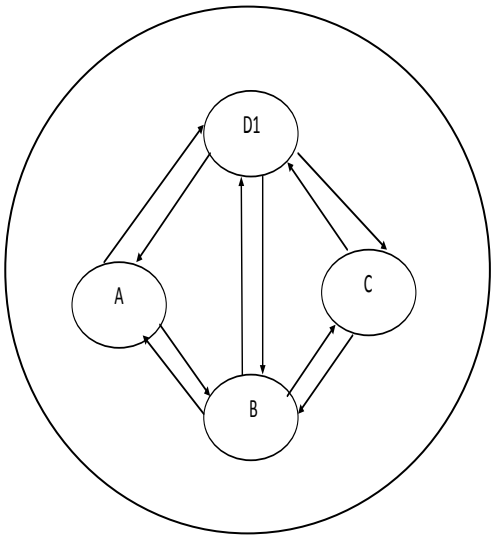
III. Advantages of Protocol

There are some key advantages using propose Inter Domain protocol. Advantages are listed below:

1. Using user identity (called anonymity).
2. Nonce – using for anti reply attack.
3. Provides data integrity and confidentiality.
4. Users are authenticated by their home domain.
5. Establishment session key for particular session.
6. Updated identity after each session by the home server.

IV. Case Study

There is only one mobile service domain and has an authentication server. The authentication server is denoted by D1. Assume there are three mobile users A, B and C, each one is registered with D1. If A, B and C wants to communicate securely with each other then they have to follow the steps below.



Step 1 : A send a request to his home (D1) server that A wants to communicate with B and C.

Step 2 : After verifying request D1 is looking for B and C's home domain and determine that B and C are in the same home domain. Now D1 generate a session key K_{ABC} and send to B along with B's new identity for future communication.

Step3 : Now B confirms to D1 that B is ready to communicate with A and C.

Step 4 : D1 talks to C that A and B want to talk to you; then D1 sends session key K_{ABC} along with new identity of C.

Step 5: C confirms to D1 that C is ready to communicate with A and B, and send identity along with response.

Step 6 : D1 send session key with identity of both B and C to A and A's new identity.

Step 7 : A, B and C can communicate securely.

V. Conclusion

We are all aware of the growth in routing complexity, and the rapid increase in allocation of network numbers. So, we need some setup rules for secure communication between end-to-end machines. In Inter-Domain Routing Protocol (IDRP) provides secure routing for OSI defined network environments, which is similar to BGP in the TCP/IP network. The Border Gateway Protocol (BGP) provides a standard mechanism for inter-domain routing among heterogeneous domains, called autonomous systems (AS), here each domain has the administrative control over its intra-domain routing protocol and inter-domain routing policy, which is not known to the other domains.

References References Referencias

1. http://www.webopedia.com/TERM/S/symmetric_key_c ryptography.html
2. http://en.wikipedia.org/wiki/Inter-domain
3. http://www.freepatentsonline.com/7240366.html
4. https://wiki.internet2.edu/confluence/download/attachments/19074/IDC-Messaging-draft.pdf
5. http://en.wikipedia.org/wiki/Anonymity
6. http://en.wikipedia.org/wiki/Cryptographic_nonce
7. http://www.networkdictionary.com/protocols/idrp.php
8. http://en.wikipedia.org/wiki/Session_key
9. http://en.wikipedia.org/wiki/Universal_one-way_hash_function
10. http://www.ist-intermon.org/download/IM-WP3-FOKUS-CINI-Interdomain_Issues-draft.pdf

This page is intentionally left blank