International Journal of Emerging Engineering Research and Technology
Volume 2, Issue 5, August 2014, PP 35-39
ISSN 2349-4395 (Print) & ISSN 2349-4409 (Online)

Secure Key Exchange Algorithm for Delay Tolerant Networks

Yamini R[1], Thilagavathy D[2], Sakthi Nathiarasan A[3]

[1]M.E-Student, Department of CSE, Adhiyamaan College of Engineering, Hosur, India.
[2]Professor and Head, Department of CSE, Adhiyamaan College of Engineering, Hosur, India.
[3] M.E-Student, Department of CSE, Adhiyamaan College of Engineering, Hosur, India.

Abstract: *Networks where end-to-end connectivity and seamless access to nodes are not possible generally belongs to the category of Delay Tolerant Networks. Several security goals including authentication, access control and confidentiality have to be achieved. Existing security mechanisms based on Public Key Infrastructure(PKI) and Identity Based Cryptography(IBC) are not complete solutions for DTN. Since these mechanisms are most suitable for end-to-end communications. The proposed research work mainly focuses on Key Exchange Algorithm for DTN, the exchanged key can be used for subsequent Encryption and Authentication. The proposed Algorithm uses the concepts of MAC, Timestamps and Logarithmic concepts and hence it overcomes all sort of know attacks including Man-in-the Middle attack and Replay attacks.*

Keywords: *DTN, IBC, PKI, MAC, Timestamps.*

1. INTRODUCTION

Delay tolerant network is a new research area in networking, which operates in extreme environment where quality of service cannot be achieved easily. Delay tolerant network finds application in the fields of communication in rural areas where continuous seamless internet connectivity cannot be guaranteed. Normally communication between two entities in the public global internet uses TCP for reliable data transmission, in some scenarios where reliable data delivery is not needed, in such cases UDP may be used. TCP provides reliable end to end communication. For challenged environment, providing end-to-end communication is not at all possible. In such a case special protocols which takes of data delivery, support of QOS is needed. All these problems give birth to delay tolerant networking. DTN is mainly used when low latency is available for communication between two communicating entities in the network. One of the main problem in extreme networking environment is data loss problem. The main reason for this problem is due to non-availability of seamless internet connectivity. Hence delay tolerant network uses store and forwarding techniques. The reason for using this technique is to achieve reliable data delivery through data retransmission. The data can be removed from the buffer of a node only after it is delivered to the neighboring intermediate node or the destination node. Delay tolerant networks uses variable length packet as the communication abstraction and a naming syntax that supports a wide range of naming and addressing conventions to enhance flexibility. It is designed to use storage within the network. The storage will be pool of buffers which are used to support store-and-forward functionality over multiple paths and potentially long timescales, and not to require but to support end-to-end reliability. DTN is an overlay network which is more probably used in areas like communication in hilly and forest regions, underwater communication, deep-space communication and in areas where signal attenuation happens due to natural factors like snow drops. DTN has bundle layer where the data to be delivered is stored and forwarded until it is received by the destination node, instead of end to end connectivity. The DTN overlay network specifies a bundle protocol which is layered on top of a "convergence layer", which is itself on top of other lower layers. The DTN Bundle Protocol describes the format of the messages normally called as called bundles, which are passed between DTN bundle agents that participate in bundle communications to form the DTN store and forward overlay network. Several security goals have to achieve in DTN. Existing techniques including PKI, IBC are not fully effective for DTN. Our research article focuses on effective key exchange algorithm based on MAC and logarithm concepts for DTN.

2. Basic Concepts

2.1 Bundle Protocol

In delay tolerant network, messages are transmitted in the form of bundles. These bundles are passed over traditional internet protocol (IP) packets. The message bundle consists of destination identifier filed which is used to identify the destination node in the delay tolerant network. Bundle protocol acts as interface between higher level application layer protocols and lower level transport layer protocols that are mainly used for message forwarding. The reason for using bundle protocol is to implement store and forward approach for forwarding data packets.is implemented in delay tolerant network by bundle protocol

2.2 Space DTNs

DTN over space will make a real network environment. DTN over space will have huge delay in data transformation. The bundle protocol transforms information with internet by native internet protocols. Convergence Layer adapter (CLA) acts as interface between the bundle protocols. Bundle protocol identifies the bundles by the bundle endpoint id. The data unit in bundle protocol is the bundles and the bundle node can transform the data.

2.3 Store and Forward Approach

Delay Tolerant Network suffers from the serious drawback of non-seamless internet connectivity. To tolerate against this store and forward approach is used. Each and every node present in the delay tolerant network uses store and forward mechanism for this purpose. Store and forward mechanism involves the buffer, which is used to store data packets temporarily until it is delivered to the nearby node or the destination node.

2.4 DTN’s Security

Security is one of the important factor to be considered in any network. The basic security goals to be achieved in any network is authentication, access control and confidentiality. Some form of access control and authentication mechanisms are needed in DTN in order to prevent the malicious intruder in gaining communicating messages. In DTNs, forwarding nodes are also authenticated, the forwarding nodes may be normal hosts, routers or gateways. sender information is authenticated by forwarding nodes, so that network resources can be conserved by preventing the carriage of prohibited traffic at the earliest opportunity. Confidentiality can be achieved through encryption using public key cryptography. Here Each networking entity whether the entity may be sender or receiver has a private key and public key pair. A certificate is issued by trusted third party called certificate Authority (CA). the certificate authority digitally signs the certificate. The certificate will be used for authentication purposes i.e., to confirm the user’s identity. Here the source node sends its bundle, together with its bundle specific signature to an adjacent forwarding node. If it does not have the copy of the sending node’s certificate, then it receives it from either certificate authority or sending node. The forwarding node or intermediate node first receives the sender’s bundle and verifies the sender’s identity, replaces with their own identity and then forwards the packet. In DTN each node verifies only the neighbor’s identity and by this way authentication can be achieved. Confidentiality can be achieved by public key encryption. Here each entity encrypts with its own private key and receiving entities decrypts with their public key. By this way DTN messages can be protected from third party masquerading.

3. Existing Techniques

3.1 Initially Public Key Infrastructure (PKI)

PKI is mainly used for the authentication purposes. Here certificates are used to authenticate a user. Certificate authority is the central person who takes care of creation, signing the certificate. A certificate can be verifiable by any node present in the delay tolerant network. A dynamic repository is also maintained by certificate authority to maintain the list of certificates along with functionality. Hence one user can authenticate over another user's public key by certificate signed by the certificate authority (CA). This PKI is implemented by online certificate revocation list (CRL) posted by CAs. Then the register authority (RA) can promote a verity of administrative process from CA. Finally repository is used to store the certificate and CRL. In this situation if there is no internet connection then receiver cannot authenticate sender's public key or certificate the DTN. PKI is not the right security mechanism for DTN communication. DTN will have no end to end connection and the implementation of PKI is impossible in this network.

3.2 Identity Based Cryptography (IBC)

IBC is public key cryptography scheme used for authentication and integrity, here the string is considered to be a valid public key. The sender sends the message to the receiver by encrypting the message using the receiver's public key. While the receiver receives the encrypted message the receiver contact to the Private Key Generator (PKG) who is a third party to obtain the decrypted message. Here Sender generates the random key and sends the cipher text 'c' and envelope 't '. Then the generated 'c' and 't' values are passed to the the receiver. PKG is the interface between sender and receiver. Where private key's' and also generate 't' (i.e. encryption of symmetric key with shared key). Then symmetric secret key ' t' is passed to the receiver. Now Receiver gets' t' from the PKG and decrypt the message. IBC is considered to be undesirable network because of intractable problem over PKG parameter, private key revocation and name space management. Bhutta et al., analysed the security mechanism and concluded that single key management is not possible due to overlay of DTNs over heterogeneous network.

4. Proposed System

In our Proposed key exchange algorithm, only the sender and receiver is involved in key generation. No centralized entity involves in key generation . we introduced logarithmic techniques and timestamps to prevent Replay attacks by malicious nodes. The proposed technique is as follows:

Suppose Alice(A) wants to exchange key with Hui(H).

Both A and H use 'e' as a secret number as the base of log.

Step 1: A chooses a large prime number M and

calculate K1=log e(M).

Step 2: H chooses a large prime number N and
calculate K2=log e (N).

Step 3: A calculates MAC(K1), secret key for MAC
Calculation is 'e'.

Step 4: H calculates MAC(K2), secret key for MAC
Calculation is 'e'.

Step 3: A sends K1 ,Timestamp T1 and MAC(K1) to H.
Step 4: H sends K2 ,Timestamp T2 and MAC(K2) to A.
Step 5: At A:

(i)calculates MAC(K2) and verifies with sender’s MAC(K2)

(ii)Verifies Timestamp ‘T2’

(iii) calculatesKey S=K1+K2

S=log e (M) + log e (N) = log e (MN).

Step 6: At H:

(i)calculates MAC(K1) and verifies with sender’s MAC(K1)

(ii)Verifies Timestamp ‘T1’

(iii) calculates Key S=K2+K1

S=log e (N) + log e (M) = log e (NM).

Step 7: By the properties of logarithms log e (NM) =log e (MN).

Both A and H can check whether the key is being attacked or not by calculating as follows: e^log e (MN)=MN. A calculates R1=MN/M If R1 is a prime number then key is not attacked. Similarly H calculate R2=MN/N. If R2 is a prime number then key is not attacked. The purpose of using MAC is to ensure that key exchange is free from Authentication attacks.

5. Security Analysis

5.1 Selection of ‘e’

Selection of ‘e’ ultimately determines the security of the algorithm. An effective ‘e’ value can be selected by choosing a prime number using random number generator called miller- rabin random number generator. First a random odd number is chosen and is validated and set of tests are conducted, if the number passes ‘n’ tests, it is said to be a effective unpredictable prime number.

5.2 Calculation of MAC

The value of ‘e’ which is shared by both sender and receiver is used as key for MAC calculation. The effectiveness of the MAC makes our proposed algorithm to withstand against deny sending/receiving attacks by one of the communicating parties.

5.3 Elimination of Man-in-the-middle Attack

Note that both H and A use a secret number ‘e’ as the base of the log. If in the middle the key is attacked and the key is changed not necessarily the base will be ‘e’. As we can calculate R1=MN/M and R2=MN/N so we can easily catch the error.

5.4 Elimination of Replay Attacks

Replay Attacks are not all possible due to the use of timestamps. An opponent can replay a message but both ‘A’ and ‘H’ may check timestamps before calculating key in order to detect Replay Attacks.

6. Conclusion

Extreme environments where achieving seamless connectivity and end-to-end connectivity is not completely possible are generally said to be delay tolerant networks. in such an environment, security is an important concern to be achieved. Authentication and confidentiality are the two primary goals to be achieved. Key management is a first step to achieve both the security goals. Traditional PKI and

IBC exhibits several drawbacks. The proposed key exchange algorithm uses logarithms, MAC and timestamps to prevent all the known attacksincluding man in the middle and replay attacks.

REFERENCES

[1] Priyanka Goyal, Sahil Batra, and Ajit Singh. "A literature review of security attack in mobile ad-hoc networks". International Journal of Computer Applications, 9(12):11–15,November 2010.

[2] Hai Huang and Zhenfu Cao. "An ID-based authenticated key exchange protocol based on bilinear Diffie–Hellman problem". Department of Computer Science and Engineering, Shanghai Jiaotong University,ASIACCS, 2009.

[3] Jooyoung Lee and Je Hong Park. "Authenticated key exchange secure under the computational Diffie–Hellman assumption".The Attached Institute of Electronics and Telecommunications Research Institute, Korea, IACR, 2008.

[4] ElGamal T. "A public-key cryptosystem and a signature scheme based on discrete logarithms", IEEE Transactions on Information Theory, volume 31, pages 469-472. 1985.

[5] Francois J., Raymond A. "Seurity Issues in the Diffie-Hellman Key Agreement Protocol", IEEE Trans. on Information Theory, pages 1–17 ,1992.

[6] K. Fall, "A Delay Tolerant Networking Architecture for Challenged Internet," In: Proceedings of the 2003 con-ference on applications, technologies, architectures, and protocols for computer communications, SIGCOMM' 03, Karlsruhe, 2003, pp. 27-34.

[7] A. Kate, G. Zaverucha and U. Hengartner, "Anonymity and Security in Delay Tolerant Networks," The 3rd In-ternational Conference on Security and Privacy in Communications Networks and the Workshops, Secure Com-munication, September 2007, pp. 504-513.

[8] X. Lin, R. Lu, C. Zhang, H. Zhu, P.-H. Ho and X. Shen, "Security in Vehicular Ad Hoc Networks," IEEE Com-munications Magazine, 2008, Vol. 46, No. 4, pp. 88-95.

[9] R. Lu, X. Lin, H. Zhu, P.-H. Ho, X. Shen, "ECPP: effi-cient conditional privacy preservation protocol for secure vehicular communications," The 27th IEEE International Conference on Computer Communications, INFOCOM 2008, Phoenix, 15-17 April 2008.

AUTHORS' BIOGRAPHY

R. Yamini received the B.Tech degree from Adhiyamaan College Of Engineering, Hosur in the year of 2012 . She is currently doing her M.E in Computer Science and Engineering in Adhiyamaan College of Engineering, Hosur. Her area of interest are Cryptography and Network Security, Real time Software Development and Sensor Networks. She is an active member of CSI.

Dr. D. Thilagavathy M.E., Ph.D is working as professor & head in the department of Computer Science and Engineering in Adhiyamaan College of Engineering, Hosur, Tamil Nadu, India. She obtained her Ph.D Degree from Anna University Chennai in the year 2012 and obtained her P.G Degree from Sona College of Tech – Salem in the year of 2004. She is having an experience of about 15 years and published about 20 paper in various international journals and have presented about 30 papers in national conferences. Her area of interest includes Key Agreement, Key Distribution in Network Security, Information Security and Mobile Security. She is a life member of ISTE.IE(I), CSI.

A. Sakthi Nathiarasan received B.Tech degree in Information Technology from Sri Krishna College of Engineering and Technology, Coimbatore, India in the year of 2013. He is currently doing his M.E degree in Computer Science and Engineering in Adhiyamaan College of Engineering, Hosur and he published 8 research articles in international journals and conferences. His area of interests includes Wireless Ad Hoc Networks, Cryptography and Network security, Utility Mining, Genetic Algorithms and Autonomic Computing. He is an active member of CSI.