© 2015 IJSRSET | Volume 1 | Issue 1 | Print ISSN : 2395-1990 | Online ISSN : 2394-4099
Themed Section: Engineering and Technology

Authenticated Key Exchange in DTNs using Public Key Exchange

Yamini. R[*1], Dr. Thilagavathy. D[2]
[*1,2] Department of Computer Science and Engineering, Adhiyamaan college of engineering Hosur, Tamiladu, India.

ABSTRACT

Data is accessed in a network with high authentication in network security. Delay Tolerant Network (DTN) is overlaid over network to communicate in rural areas, space etc. DTNs forward data by store and forward technique. But due to dis-connectivity this transmission of data is not transmitted securely. To avoid dis-connectivity and to have secured communication Time Evolving and Two Channel cryptography are implemented with RSA based key Exchange.

Keywords: Delay Tolerant Network, Bundle Protocol, Time Evolving, Two Channel cryptography, Key Exchange.

I. INTRODUCTION

Network security is an important aspect for transmission of information or data from sender to receiver. This exchange of data from sender to receiver is authenticated. Authentication in a network is based on public and private key exchange. Example if a user sends a secret message to the receiver using the public key of the receiver (i.e. mailed) and the receiver can view the message using its own private key (i.e. password). In delay tolerant, the secured communication is considered in network security [1]. Hence DTNs itself faces number of issues and hence considering the issues secured communication is established here.

A. Delay Tolerant Networks

Delay Tolerant Network was mainly suggested to have continuous connection in heterogeneous area. DTN network is also defined as "Network of the Regional Networks" since it overlay over the regional networks [2]. Hence, End-to-End connectivity is not possible. DTN can be implemented as Hop-to-Hop Networks. Communication in DTN can be made through Bundle Layer and not in TCP/IP. But the main disadvantage of DTN is dis-connectivity and delay.

B. Bundle Layer Protocol

This layer is intended to function above the existing protocol layers and provide the function of a gateway when two nodes come in contact with each other. In DTN, the node is identified as an entity with "bundle layer". The node will act as a host, router or a gateway. Host can receive data but it will not forward. Router can forward data but with single DTN region. Whereas gateway can forward data with two or more DTN region.

C. Store-and- Forward Technique

Store and forward technique is implemented in bundle layer. Here data is forwarded only if there is link to another node for receiving the data [2]. Else the data is stored in the database until a path exists between two nodes. With this technique of data transmission data is never lost when dis-connectivity take place.

II. LITERATURE REVIEW

In the year 2003, Kevin Fall as proposed an authenticated key exchange in Delay Tolerant Network. His idea is based on Public Key Infrastructure (PKI) [3]. Applicant will generate the key pair and pass that to the registration authority. The RA will send a certificate request to the certified authority. Then CA will generate certificate and forward it to the certificate revocation list here the certificate are encrypted by digital signature. This digital is then forwarded to applicant by RA. Drawback over it is If End Entity trusts unknown PKI

domain irresponsibly, and then its issuer CA cannot apply their security policy to the End Entity.

In the year 2008, Rabin Patra, Sonesh Surana, Sergiu Nedevschi proposed hierarchical identy based cryptography for authenticated key exchange. Here public Key Generator (PKG) technique is used for key exchange purpose [4]. Hence PKG generate global key and a master key, Global is public key distributed to all. PKG uses master key to generate private key corresponding to the public key ID of the receiver. Sender encrypts the message using public key ID from the receiver. Receiver decrypt message private key generated by PKG. the problem identified here is dis-connectivity, due to which data loss will take palace. Once data is loosed there is no authenticated data transformation.

In the year 2010, William L. Van Besien suggested the idea of Bundle Security Protocol over DTN. The specification describes IPsec style security headers [5]. **Bundle Authentication Block:** Authenticate the data between two neighbour node using certificate and message authentication is made by HMAC-SHA1 algorithm. **Payload Integrity Block:** End to End data integrity is made possible by RSA digital signature. **Payload Confidentiality Block:** Encrypt the data in whole or part from source to destination using AES encryption. **Extension Security Block:** It prevent the non-payload block that not related to payload using RSA-AES128 Attacks here is Packet dropping attack , Address spoofing attack.

In the year 2010, Minsu Huang, Siyuan Chen, Ying Zhu, Yu Wang proposed cost efficient topology design problem in a predictable delay tolerant networks (DTN) where the time-evolving network topology is known a priori or can be predicted [6]. It uses Space-Time graph and Greedy algorithm to detect the path earlier. This technique will be highly useful to identify the path between two nodes earlier and delay can be reduced. The problem over this technique is there is no authenticated data transformation.

In the year 2012, Zhongtian Jia, XiaodongLin, Seng-HuaTan, LixiangLi, YixianYang proposed the idea of distributing public key in DTN with the use of Two Channel cryptography [7]. Data is transmitted in two channels for secured data travelling. Broadband channel is unsecured channel because nodes in between two nodes can plays a major role, which can modify the data transmitted by the source. Narrowband channel will transmit data with high authentication, by generating hash values to the data. Here authenticated data transmission will take place but suffers by dis-connectivity.

III. EXISTING WORK

Data is transmitted in a DTN through time evolving technique and Two Channel cryptography with Diffie-Hellman based key exchange. Time evolving [6] will point when and to whom the data should be forwarded. Two-Channel Cryptography [7] will have an authenticated data transmission with non-interactive key exchange. This Diffie-Hellman key Exchange [8] will have adversary node acting over it. First to identify the path in DTN Time Evolving technique is proposed this technique is implemented with Space-Time graph and Dijkstra's algorithm. Space and time graph will show the distance between two nodes and the time taken to send the public key. Once the key is received by the next node the path of transmitting the data can be identified and the then the data is being transmitted to the next node. With respect to time the path is being identified and the data is transmitted. Figure 1 shows the path established with different time.

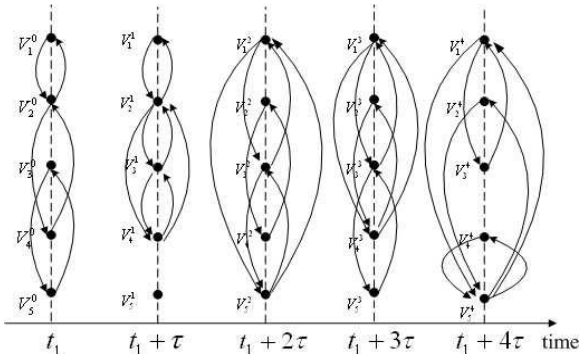

Figure 1: Space-Time graph

For transmitting the data with nearest path Dijkstra's algorithm is used to find the shortest path and the path is generated without cyclic path. Figure 2 shows the acyclic shortest path for data transmission.

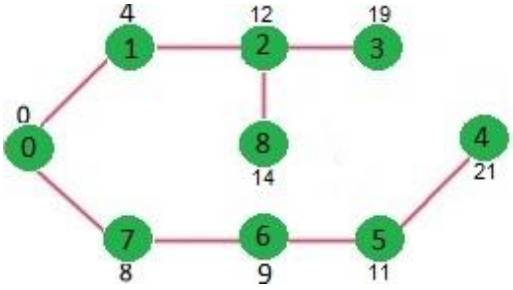

Figure 2: Shortest path

After finding the path the data is made authenticated by using Diffie-Hellman key Exchange. Here even though the data is authenticated, due to pre- authentication of data and transmission of secrete key through the adversary node will have man-in-the-middle attack. There are two channels here the broadband is used for transmitting the pubic key. And the narrowband is used for transmitting the secrete key which is converted to hash values for security propose. The main drawback of the existing results in man-in-the middle attack.

IV. PROBLEM IDENTIFICATION

In DTN secured communication is lacking by using Diffie-Hellman key exchange. Data is transmitted through adversary nodes and hence Man-in-the-Middle attack may take place. Designing a Secure Key Exchange Algorithm which will handle Man-in-the-Middle attack.

V. PROBLEM SOLUTION

To avoid dis-connectivity and delay Time-Evolving and Two-Channels cryptography is being implemented. RSA based key exchange will provide highly secured data transmission, because here the private key is never need to be transmitted.

VI. PROPOSED WORK

The proposed work overcomes Man-In-The-Middle attack that is being identified in the Diffie-Hellman key exchange. Hence RSA based key exchange [9] will encrypt the key send by the sender by using the public key and decrypt the key by the destination by using the private key. This is implemented with Two-Channel [6] and Time-Evolving Technique [7]. In RSA the message can be encrypted without the without the need to exchange a secret key. The RSA algorithm is mainly used for public key encryption. The security of RSA is based on the difficulty of factoring large integers. Source node can send an encrypted message to destination without any prior exchange of secret keys. Sender will just use the receiver's public key to encrypt the message and receiver will decrypt the message by using its own private key, which is known only to the receiver. RSA can also be used to sign a message, so sender can sign a message using their private key and receiver can verify it using sender's public key. The key generation in public is made as following.

1. Select two prime number (p, q) and both p and q should not be equal.
2. Then calculate n with respect to product of p and q.
3. Calculate the φ value by p-1 product of q-1
4. Select a integer e (i.e. gcd(φ,e)=1) which is relatively prime to φ and it is less than φ.
5. Determine d value using ($d \equiv e^{-1} \bmod \varphi$)
6. Public key and private keys are generated as e, n and d, n respectively.
7. A plain text is encrypted using the public key by $C= M^e \bmod n$.
8. A cipher text is decrypted using the private key $M= C^d \bmod n$

VII. CONCLUSION

An adversary node plays a major role in Diffie-Hellman key exchange. Adversary node can entirely change the secret key transmitted by the source node to destination node. Hence Diffie-Hellman key exchange suffers from Man-in-the-middle attack. To overcome this man-in-the-middle attack proposed work is implemented with RSA algorithm. RSA (Rivest-Shamir-Adlemen) based key exchange algorithm will provide highly authenticated data transmission. Because here the data is transmitted securely by encryption and decryption.

VIII. REFERENCES

[1] V. Cerf, S. Burleigh, A. Hooke, L. Torgerson "Delay-Tolerant Networking Architecture"NetworkWorkingGroup Google/Jet Propulsion Laboratory, April 2007
[2] Artemios G. Voyiatzis, Member, IEEE "A Survey of Delay- and Disruption-Tolerant NetworkingApplications" Journal of Internet Engineering, Vol. 5, No. 1, June2012
[3] Fall, K.. "Adelay-tolerant network architecture for challenged internets", SIGCOMM'03: Proceedings of the2003 conference on Applications, technologies, architectures, and protocols for computer communications,ACM, New York, NY, USA, pp. 27–34. 2003
[4] R. Patra, S. Surana, and S. Nedevschi, "Hierarchical identity based cryptography for end-to-end security in DTNs," in Proc. IEEE 4th Int. Conf. ICCP, Aug. 2008, pp. 223–230.
[5] W. Van Besien, "Dynamic, non-interactive key management for the bundle protocol," in Proc. 5th ACM Workshop Challenged Netw., 2010, pp. 75–78.
[6] M. Huang, S. Chen, Y. Zhu, and Y. Wang, "Cost-efficient topology design problem in time-evolving delay-tolerant networks," in Proc. IEEE Global Telecommun. Conf., Dec. 2010, pp. 1–5.
[7] Z. Jia, X. Lin, S. Tan, L. Li, and Y. Yang, "Public key distribution scheme for delay tolerant networks based on two-channel cryptography," J. Netw. Comput. Appl., vol. 35, no. 3, pp. 905–913, May 2012.
[8] http://crypto.stackexchange.com/questions/14508/diffie-hellman-key-exchange-with-authentication-man-in-the-middle-query
[9] http://www.internet-computer-security.com/VPN Guide/RSA.html