Advances in Parallel Computing Technologies and Applications
D.J. Hemanth et al. (Eds.)

doi:10.3233/APC210130

Trust-Based Public Key Management for Data Distribution in Wireless Networks

Sivaprakasam T [a,1]
[a] *Lecturer, Department of Computer Engineering, Alagappa Government Polytechnic College, Karaikudi, India*

Abstract. A packet has to be delivered within a distinct time limit as data delivery is a critical issue in a wireless network. In emergency situations, real-time data distribution of multimedia file is addressed using wireless network. The real-time data examined here are image and audio files and these files are broken into sequence of packets and forwarded to the destination peer node based on a Priority algorithm. Prioritized data dissemination processes the sequence of packets to be forwarded based on permanent priority scheduling. The packets are encrypted based on Trust-based Public key management using public key generated in key generation phase and decrypted at the receiver end. The simulation results prove that the proposed technique has the enhanced and secured data transmission. The design of the network requirements and detailed experimental results are presented.

Keywords. Trust, Public key, private key, key management, data distribution, wireless networks.

1. Introduction

A network is a collection of mobile devices that must have the communication into the wireless medium that could not generate the common infrastructure [1]. The devices have been facilitated an enhanced communication with the internet according to the latest capability and minimized cost to permit the utilization of sever network type without any fixed framework [2]. The wireless network has the independent framework that is fixed and the mobile nodes should communication through adjacent nodes within the transmission range [3]. The resources are shared among the interconnected nodes without the use of centralized administration is a benefit of wireless network. Many application domains use wireless networks and the technologies used in wireless networking include GPRS, Bluetooth, and WLAN etc [4]. In order to sustain a permanent connection even when the nodes are mobile, it is an important task to analyze the wireless technology usability and handover experienced [5]. In wireless network each node is referred as node and it follows a fully decentralized architecture. Requests can be initiated by a main node to another adjacent node, likewise the main node could respond to requests incoming from other nodes connected in the wireless network [6]. Wireless networks are of great use for efficient file sharing, data sharing and downloading. To avoid any leakage

[1] Sivaprakasam T, Department of CSE, Alagappa Government Polytechnic College, Karaikudi, India.
E-mail: tsivaprakasam@gmail.com

of sensitive data or personal information security adequate security measures must be implemented [7].

2. Related works

In RSA Algorithm [8], a key utilized for encryption shouldn't be used for other purpose, because if the key is cooperated the entire information disclosed is exposed to risks. Moreover if the single key is compromised, then the information cannot be decrypted at receiver side. An enhanced method related to the public key enabled security [9], the similar format is utilized to secure the useful files. The procedure for implementing the authentication process should be achieved through the signature enabled methods. The security related problems have been solved through the complexity function to reflect higher execution period. The RSA enabled methodology [10] has been implemented the security through the increment of the security side; the execution period has been reduced compared with related techniques [8]. Whenever the execution period of the RSA technique has been solved the issue of bottleneck while performing in real-time application that the minimization of the execution period needed to utilize the technique for several purposes [11,12]. The decryption process has been utilized the time reduction which has the private components of modular computation. The multi-prime related technique [13] has been used the key generation process to generate the prime values. The other cryptographic techniques are implemented for providing security as dynamic trust routing [14,12], intelligent secured mobility estimation [15], group key generation [16], and threshold multi-authority access [17].

3. Typographical style and layout

Data distribution is used in dissimilar keys that are utilized for encryption and decryption in public key cryptography hence the process is called as an asymmetric system. Combining the public key with its certification by means of digital signatures protocols enhances the authentication and integrity of data. Network with high bandwidth and low cost allows users to exchange multimedia content which may be image data, video, audio etc. Thus the necessity for encryption and decryption comes into picture. Transmission of real-time data includes multimedia communication hence huge amounts of audio, video, image must be transmitted in a secure manner. The multimedia content needs to be transmitted in timely manner as well as the quality of the communication must be guaranteed. The content is streamed directly to the receiver by active sender and the nodes which are capable to stream the same content anytime are standby senders. Based on the active sender's availability and congestion in network path the scheduling is commenced. A standby sender replaces the active sender when congestion raises overmuch or an active sender fails. The limitation of the above scheme is that there is need for particular network layout in the case of mobile environment. A folder is created for all the mobile nodes in wireless network involved in the data dissemination process. Each folder corresponding to the node contains data files such as image or audio. Folder represents storage space to store data specific to a device. The file transfer is demonstrated in Figure 1.

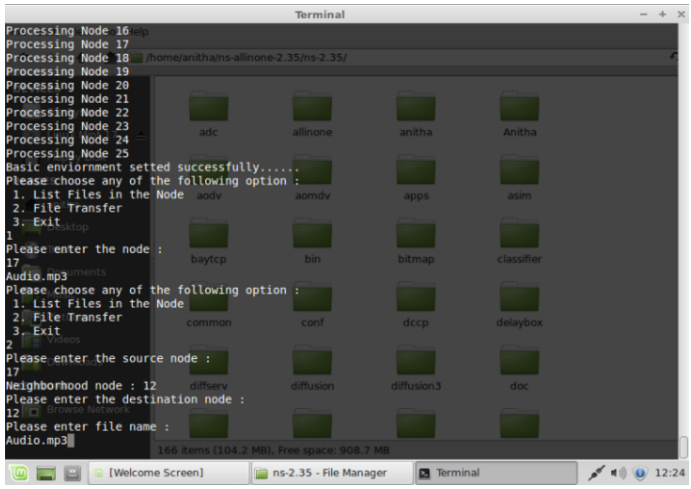

Figure 1. File transfer

3.1. Trust-based Public key management

Each node requires generating a certification with valid key pair where the public key must be delivered frequently. The digital signature technique is implemented to calculate the key pairs. The NTC based key pairs have been generated randomly whenever a node discovers its equivalent NTC, the node needs that NTC to perform the certification process and the public key has been generated. According to the availability of the trust value from the profile, the NTC performs the delivery of the certificate for the key pair to the node due to the condition. For assumption if there are 25 nodes connected in MANET environment, there is folder created for each node. Each folder corresponding to the nodes represents the storage space for the files involved in transfer.

3.2. List Files

The List File method lists all the files in the folder of the respective node. The pseudocode for listing files in a node is given below: The certificate package demonstrates the node

Algorithm 1 File Listing

```
1: set f [gets stdin]
2: if f <=n then
3:     set dir "$envName/$f/"
```

public key certificate that is delivered through the digital signature of NTC within the execution period. Whenever the termination time is reached, the node needs to upgrade the key value for providing the security. The trust threshold value maintains the enhanced performance for implementing the security as each node generates its key pair which is normally a huge random value and it is securely managed. The unique key has been generated for each node with the certificate confirms the generated valid keys, the entire process is demonstrated in Figure 2.

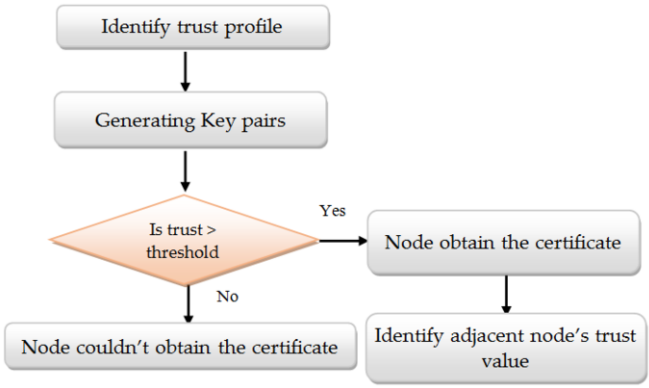

Figure 2. Process of Trust-based key management

3.3. File Transfer

The File transfer method gets the user choice of which file has to be transferred. If the file does not exist then file transfer operation could not take place and if file to be transferred exists then the file could be transferred if and only if the sender node has the receiver node's public key. Moreover if the nodes are untrustworthy any kind of operation could not take place. The pseudocode for file transfer is given below:

Algorithm 2 File Transfer

```
1: set fn [gets stdin]
2: set ff [glob -path $dir $fn]
3: set fName [file tail $item]
4: set fsize [file size $item]
5: puts "file Sixe : $fsize"
6: set chunk [expr $fsize/10]
```

The file to be transferred is first converted to binary file. The binary file is encrypted using RSA encryption function and converted to cipher message and then transmitted to the receiver side. To convert to binary format the code is as follows:

fconfigure $fp -translation binary
fconfigure $fo -translation binary.

4. Fine tuning

The performance of trust based public key management for real-time data distribution is evaluated for varying metrics namely Information Risk, Throughput and Transfer Speed. The performance evaluation is implemented through the simulation environment of NS2. The encryption time is calculated by Input file size divided by Encryption execution time. Likewise the decryption time is calculated by Encrypted file divided by Decryption execution time. The unit for transfer speed in KB/Sec. The average of Encryption and Decryption time gives the Transfer speed.

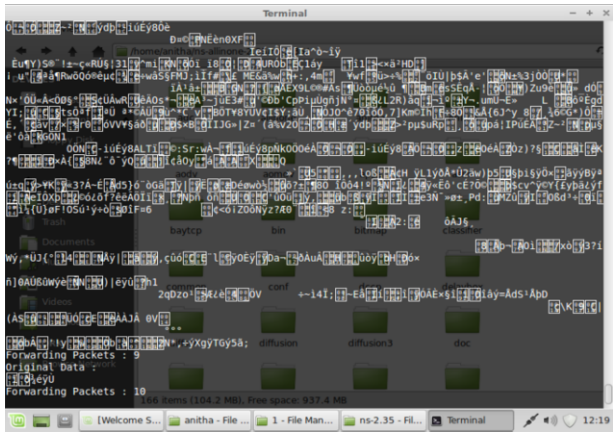

Figure 3. Encryption Process

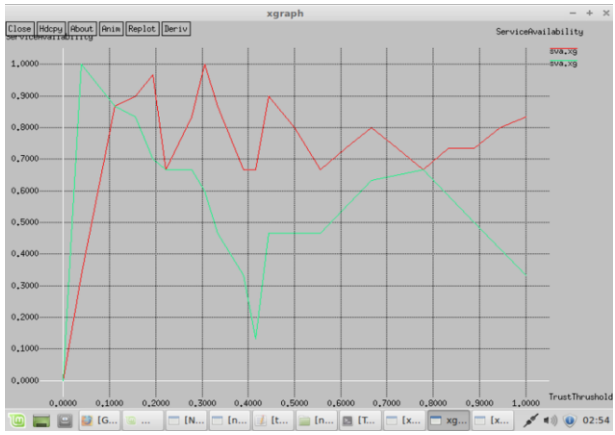

Figure 4. Information Risk

The public key is reserved in every transmission for delivering messages to the recipient node. The image encrypted at the sender side should be exactly decrypted at the receiver end. Trust-based Key Management algorithm encrypts the image/audio files with good accuracy. The throughput is the quantity of information transmitted effectively from source place to recipient place in a given time duration. The input file is partitioned into chunks of packets and each data packet has to be transferred within the limited bandwidth. Throughput is defined by Number packets partitioned from Input File size divided by Total number of Packets. Figure 3 demonstrates the encryption process of the image and audio files for transfer. Figure 4 illustrates the Information risk in every parameter related to the security. Trust bias demonstrates the dissimilarity within the node's average trust value and generated values which is demonstrated in Figure 5.

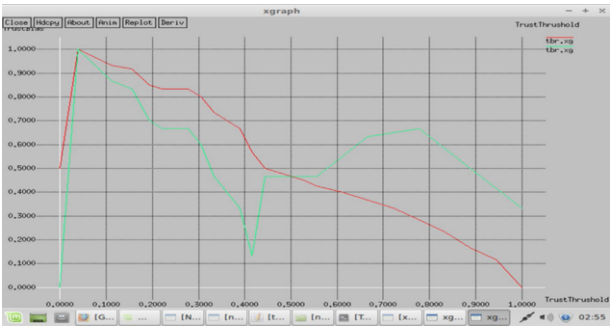

Figure 5. Trust bias

5. Conclusion

The problem of data distribution of multimedia files in wireless networks has been addressed in this paper. Data distribution of both image and audio files has been examined. Priority scheduling algorithm works based on the precedence of data packets to be implemented thus exhibiting prioritized data distribution. Its major objective is to present firm prioritization using priority as a scheduling aspect. Data is distributed and encrypted using the Trust-based public key management algorithm. Thereby wireless networks for distributing data have been calculated and evaluated.

References

[1] Cho JH, Chen R, Chan KS. Trust threshold based public key management in mobile ad hoc networks. Ad Hoc Networks. 2016 Jul 1;44:58-75.

[2] Bui BD, Pellizzoni R, Caccamo M, Cheah CF, Tzakis A. Soft real-time chains for multi-hop wireless ad-hoc networks. In13th IEEE Real Time and Embedded Technology and Applications Symposium (RTAS'07) 2007 Apr 3 (pp. 69-80). IEEE.

[3] Rao GR, Lakshmi PV, Shankar NR. A novel modular multiplication algorithm and its application to RSA decryption. International Journal of Computer Science Issues (IJCSI). 2012 Nov 1;9(6):303-9.

[4] Dhakar RS, Gupta AK, Sharma P. Modified RSA encryption algorithm (MREA). In2012 second international conference on advanced computing & communication technologies 2012 Jan 7 (pp. 426-429). IEEE.

[5] Thangavel M, Varalakshmi P, Murrali M, Nithya K. An enhanced and secured RSA key generation scheme (ESRKGS). Journal of information security and applications. 2015 Feb 1;20:3-10.

[6] Li Y, Liu Q, Li T. Design and implementation of an improved RSA algorithm. In2010 International Conference on E-Health Networking Digital Ecosystems and Technologies (EDT) 2010 Apr 17 (Vol. 1, pp. 390-393). IEEE.

[7] Ali ZU, Ahmed JM. New computation technique for encryption and decryption based on RSA and ElGamal cryptosystems. Journal of Theoretical and Applied Information Technology. 2013 Jan 10;47(1):73-9.

[8] Noh J, Baccichet P, Hartung F, Mavlankar A, Girod B. Stanford peer-to-peer multicast (SPPM)-overview and recent extensions. In2009 Picture Coding Symposium 2009 May 6 (pp. 1-4). IEEE.

[9] Nagar SA, Alshamma S. High speed implementation of RSA algorithm with modified keys exchange. In2012 6th International Conference on Sciences of Electronics, Technologies of Information and Telecommunications (SETIT) 2012 Mar 21 (pp. 639-642). IEEE.

[10] Peltotalo J, Harju J, Saukko M, Vaatamoinen L, Bouazizi I, Curcio ID, van Gassel J. A real-time peer-to-peer streaming system for mobile networking environment. InIEEE INFOCOM Workshops 2009 2009 Apr 19 (pp. 1-7). IEEE.

[11] Hwang RJ, Su FF, Yeh YS, Chen CY. An efficient decryption method for RSA cryptosystem. In19th International Conference on Advanced Information Networking and Applications 2005 Mar 28 (Vol. 1, pp. 585-590). IEEE.

[12] Zhou X, Han S, Liang Z, Yang X. Wireless sensor-based prediction of debris flow in mountainous areas and improvement of power business environment. Arabian Journal of Geosciences. 2021 Aug;14(15):1-7.

[13] Ding G, Bhargava B. Peer-to-peer file-sharing over mobile ad hoc networks. InIEEE Annual Conference on Pervasive Computing and Communications Workshops, 2004. Proceedings of the Second 2004 Mar 14 (pp. 104-108). IEEE.

[14] Sathiyavathi V, Reshma R, Parvin SS, SaiRamesh L, Ayyasamy A. Dynamic trust based secure multi-path routing for mobile ad-hoc networks. InIntelligent Communication Technologies and Virtual Mobile Networks 2019 Feb 14 (pp. 618-625). Springer, Cham.

[15] Dhanalakshmi B, SaiRamesh L, Selvakumar K. Intelligent energy-aware and secured QoS routing protocol with dynamic mobility estimation for wireless sensor networks. Wireless Networks. 2021 Feb;27(2):1503-14.

[16] Sabena S, Sureshkumar C, Ramesh LS, Ayyasamy A. Secure Trust-Based Group Key Generation Algorithm for Heterogeneous Mobile Wireless Sensor Networks. InInventive Computation and Information Technologies 2021 (pp. 127-141). Springer, Singapore.

[17] Selvakumar K, SaiRamesh L, Sabena S, Kannayaram G. CLOUD COMPUTING-TMACS: a robust and verifiable threshold multi-authority access control system in public cloud storage. InSmart Intelligent Computing and Applications 2019 (pp. 365-373). Springer, Singapore.