Creating Associated Digital Signature System and Applications

Thulasipriya. K[1] Dr. Thilagavathi. D[2]
[1]PG Scholar [2]Professor & Head of Dept.
[1,2]Department of Computer Science & Engineering
[1,2]Adhiyamaan College of Engineering, Hosur, India

Abstract— It is important to secure the data while transition in wireless network. Many routing available in wireless network. If a node want to send the data packets to destination means it firstly sent to neighbour node then it will reach destination. Sometimes it may cause some routing problems and vulnerability in secure systems. In order to achieve better routing with high security we propose cluster based data transmission technique. All the nodes in our network formed in to some groups which is called cluster. Cluster head is selected based upon the election algorithm. To support scalability, nodes are often grouped into disjoint clusters. Each cluster would have a leader, often referred as cluster head (CH).A CH is responsible for not only the general request but also assisting the general nodes to route the sensed data to the target nodes. For these multi certificates PKI (MCPKI) which supports user self-services, such as certificates spontaneous substitution as well as self-reissue after self-revocation. We concentrate on both RSA and digital signature for verifying the nodes trustworthiness. Our simulation results shows that the proposed RSA cryptographic technique provides high level secure transmission than existing system.

Key words: Cluster, Election Algorithm, Multi Certificate PKI, Self-Services, Self-Revocation

I. INTRODUCTION

A wireless sensor network (WSN) is composed of a large number of low-cost and low-power wireless sensor nodes. They are deployed in the specified area and form a wireless network by way of self-organizing. They can work normally at a wicked or special environment that people cannot close. This technology has been widely used in the industry, military, environmental monitoring, and medical and other fields. These nodes can be deployed easily, but they can only use the battery, and it is difficult to change the battery, so how to prolong the life cycle of the whole network is one of the hot research topics in WSN.

WSN routing protocol is responsible for looking for a data transfer path in the network layer. The data packet from the source node is forwarded to the data-receiving node by way of multi-hop communication on this path. For these characteristics of the nodes in network, like random deployment, limited energy, self-organizing, and frequent changes in network topology, there are better adaptability and energy efficiency by using a hierarchy routing algorithm based on clustering than using the plane routing algorithm.

A digital certificate is the combination of both encrypted message and the digital signature of the message. [23] The most widely used digital certificate is X.509 public key digital certificate. Public key alone cannot be used as a security factor. Public- key digital signature can be used in public key infrastructure to provide authentication of the public key. The digital signature can be signed by the trusted certificate authority (CA). A digital signature framework contains user's public information and the digital signature of public information signed by the trusted CA. The X.509 public key digital certificates is difficult to manage. The digital signature framework contains some public information of user such as digital driver's license, digital birth certificate, digital ID and so on.

A. Certificate Authority (CA)

CA is the individual or association that carefully signs an announcement with its private key. In PKI applications, the X.509 open key computerized testament contains an announcement, including the client's open key, and a computerized mark of the announcement. The contrast between the GDC and the current open key computerized testament is that in a GDC, general society data does not contain any client's open key.

B. Owner of a GDC

The proprietor of the GDC is the individual who gets the GDC from a trusted CA over a protected channel. The proprietor needs to figure a substantial "answer" in reaction to the verifier's tested "question" keeping in mind the end goal to be confirmed and build up a mystery session key.

C. Verifier

The verifier is the individual who challenges the proprietor of a GDC and approves the appropriate response utilizing the proprietor's open data and CA's open key.

Clustering algorithm is to divide the sensor network nodes into different clusters. Every cluster has a cluster head node, and the other member nodes send information to the cluster head node which continues to fuse and forward these data. Among them, it is the key of clustering algorithm to select a cluster head, and research about how to lower the node energy consumption by selecting the cluster head and then form a high-quality cluster has an important significance.

II. RELATED WORK

Mark D.Ryan (2014), [23]has proposed the enhanced certificate transparency and end-to-end encrypted mail model for authenticating website public keys. The proposed system reliably grasp the certificate revocation and enhance an end-to-end secured email using PKI with no trusted authorities. A new attacker model is developed for cloud computing environment, which is named as "malicious-but-cautious". An email provider provides the certificate keys without trusting the users.

U.Devisree and M.Santhi (2014) [24] proposed the cluster based certificate revocation with vindication capability (CCRVC) scheme. The certificate revocation can be introduced to improve the reliability of the proposed scheme. Clustering technique can be used to increase the performance such as throughput, delay, packet delivery ratio, life time. The certificate authority is capable of modifying

two lists such as white lists and black lists. The node accused as an attacker is maintained by the black list. The corresponding accusing node can be maintained by the white list.

Lien Harn and Jian Ren (2011) [1] proposed the Generalized Digital Certificate (GDC) concept which can be used to provide key agreement and user authentication. The trusted certificate authority (CA) signs the user public information using digital signature. The user information can be digital driver license, the information of a digital birth certificate and so on. Public key digital certificate can be simple, since the user does not contain any private and public key pair. The digital signature is known only to the owner, the user doesn't have any idea about the signature.

Wen-Tao Zhu and Jingqiang Lin (2016) [10] proposed the adaptable framework to generate correlated digital certificates. Later, it can be implemented to support the multi-certificate public key infrastructure which supports self-reissue and revocation. Certificate correlation tree framework can be generated using data structures. RSA public key cryptosystems has been used to adopt in public key infrastructure.

Chaum and Antwerpen (1989) [16] presented the thought of an evident mark, which empowers the underwriter to have a finish control over his/her mark. The check of an evident mark requires interest of the message underwriter. In any case, this game plan can avoid undesirable verifiers from approving the mark. The genuine issue of the irrefutable mark is that the endorser needs to validate the verifier before helping the verifier to approve the irrefutable signature.

A Designated verifier signature (DVS) [20] DVS gives validation of an offered message to a predefined verifier. One remarkable property of a DVS is that a legitimate DVS can be produced by the "genuine" endorser or by the assigned verifier. With this exceptional property, a DVS is unique in relation to a customary computerized signature in two perspectives. (i) Since the assigned verifier realizes that he/she didn't produce the DVS him/herself, the assigned verifier is accordingly persuaded that the DVS was created by the genuine endorser. In any case, not at all like the conventional computerized signature, which can be checked by any verifiers, for the DVS, no outsider part can decide the genuine underwriter of the DVS even with learning of the private key. (ii) A DVS gives confirmation of a given message without non-disavowal property of the customary advanced signature. A DVS can supplant the conventional computerized signature in many applications and furnish administrations with deniability.

III. METHODOLOGY

A. RSA Algorithm Key Generation

This algorithm uses the public key for encryption and private key for decryption.

- Step 1: Select two prime number p and q both p and q should be different.
- Step 2: Then calculate n with respect to product of p and q.
- Step 3: Calculate the G value by p-1 product of q-1
- Step 4: Select a integer e (i.e. gcd(G,e)=1) which is relatively prime to G and it is less than G.
- Step 5: Determine d value using (d e^{-1} mod Z)
- Step 6: Public key and private keys are generated as e, n and d, n respectively.
- Step 7: A plain text is encrypted using the public key by C= M^e mod n.
- Step 8: A cipher text is decrypted using the private key M= C^d mod n.

1) Digital Signature

a) Sender A does the accompanying

- Makes a message condensation of the data to be sent.
- Speaks to this review as a number m somewhere around 1 and n-1.
- Utilizes her private key (n, d) to figure the mark s = md mod n.
- Sends this digital sign s to the beneficiary, B.

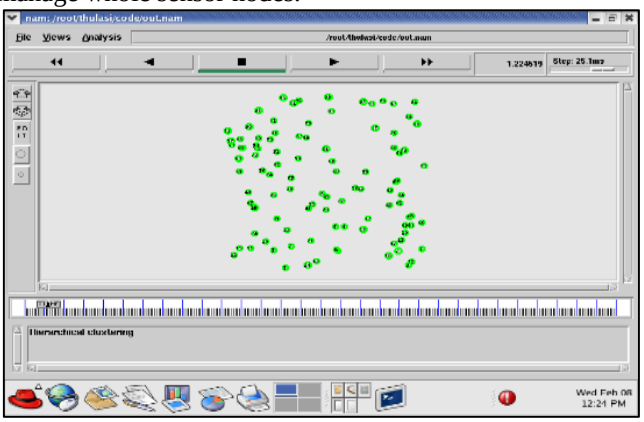
2) Verifying Signature

a) Beneficiary B does the accompanying

- Utilizes sender A's open key (n, e) to register number v = se mod n.
- Separates the message digest from this whole number.
- Freely registers the message overview of the data that has been agreed upon.
- On the off chance that both message condensations are indistinguishable, the mark is legitimate.

IV. RESULTS AND DISCUSSION

In order to achieve better routing with high security we propose cluster based data transmission technique. All the nodes in our network formed in to some groups which is called cluster. Cluster head (CH) is selected based upon the election algorithm. The node which have the highest energy is taken as CH. Clustering plays an important role for energy saving in WSNs. With clustering in WSNs, energy consumption, lifetime of the network and scalability can be improved. Because only cluster head node per cluster is required to perform routing task and the other sensor nodes just forward their data to cluster head. Clustering has important applications in high-density sensor networks, because it is much easier to manage a set of cluster representatives (cluster head) from each cluster than to manage whole sensor nodes.



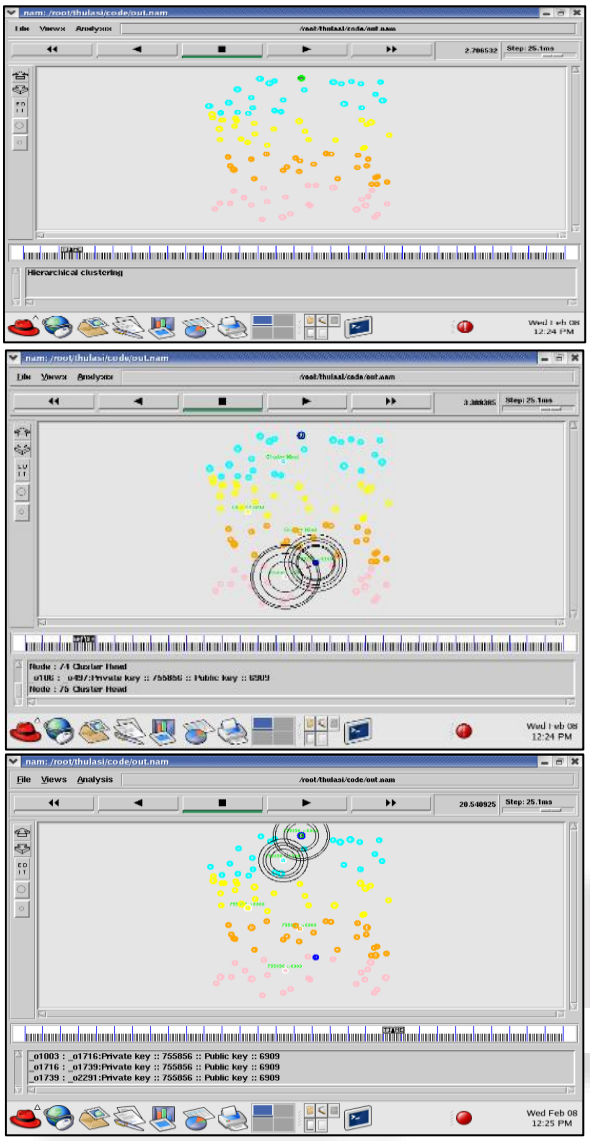


Fig. 1: Graph

100 mobile nodes can be created to forward the packets from source to destination. All nodes are grouped together to form a cluster. 25 nodes are grouped in one cluster group. The communication will be between the cluster heads. The cluster heads forward the packets from source to destination.

A. Delay

Delay is the difference between the time at which the sender generated the packet and the time at which the receiver received the packet. Delay is calculated using awk script which processes the trace file and produces the result.

$$Delay[i] = \sum_i^n (rt[i] - st[i])$$

Where

Delay[i] - denotes that the delay for each and every node which is transmit the data packet information from source to destination.

- rt[i] - Stop time
- st[i] - Start time

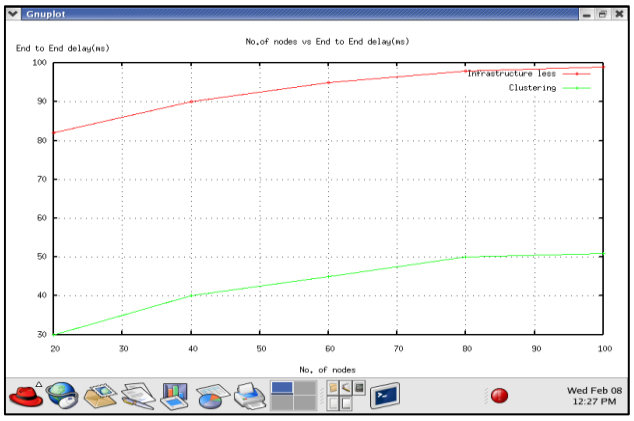


Fig. 2: Delay

B. Throughput

Throughput is the amount of work that a computer can do in a given time period. Historically, throughput has been a measure of the comparative effectiveness of large commercial computers that run many programs concurrently. An early throughput measure was the number of batch jobs completed in a day. More recent measures assume a more complicated mixture of work or focus on some particular aspect of computer operation. While "cost per million instructions per second (MIPS)" provides a basis for comparing the cost of raw computing over time or by manufacturer, throughput theoretically tells you how much useful work the MIPS are producing. Another measure of computer productivity is performance, the speed with which one or a set of batch programs run with a certain workload or how many interactive user requests are being handled with what responsiveness. The amount of time between a single interactive user requests being entered and receiving the application's response is known as response time.

$$Throughput = \sum_i^n recv\_size / (stop\_time - start\_time)$$

Where,

Recv_size - receiving size of each packets.

Start_time - the time when the nodes start to transmit

Stop_time - the time when the nodes stop to transmit

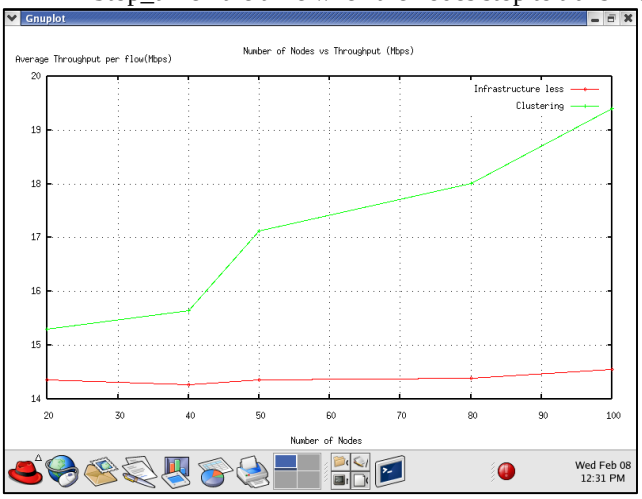


Fig. 3: Throughput

C. Packet Delivery Ratio

Many protocols in wireless sensor networks use packet delivery ratio (PDR) as a metric to select the best route, transmission rate or power.

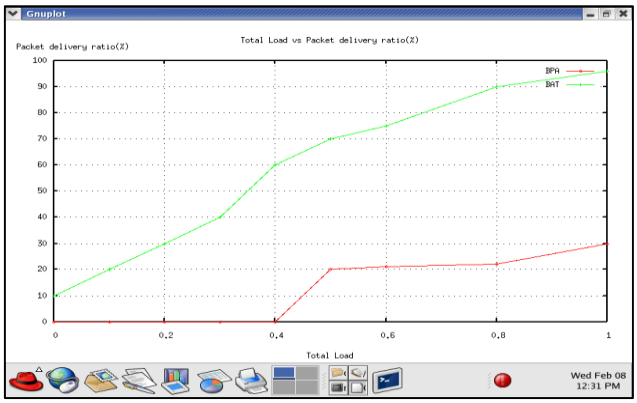


Fig. 4: PDR

V. ENERGY CONSUMPTION

Energy consumption is nothing but overall energy consumed for transmission. CE denotes the consumed energy for all nodes. Final energy is taken after sending and receiving of each node. Final energy is also called remaining energy. The energy model represents the energy level of nodes in the network. The energy model defined in a node has an initial value that is the level of energy the node has at the beginning of the simulation. This energy is termed as initial Energy. In simulation, the variable "energy" represents the energy level in a node at any specified time. The value of initial Energy is passed as an input argument. A node loses a particular amount of energy for every packet transmitted and every packet received. As a result, the value of initial Energy in a node gets decreased. The energy consumption level of a node at any time of the simulation can be determined by finding the difference between the current energy value and initial Energy value. If an energy level of a node reaches zero, it cannot receive or transmit anymore packets. The amount of energy consumption in a node can be printed in the trace file. The energy level of a network can be determined by summing the entire node's energy level in the network.

$$CE = \left(\sum_i^n \text{Initial\_Energy} - \text{Final\_Energy [i]} \right)^n$$

Where,

CE - Consumed Energy

i - Initially i is 0

n - Number of nodes

Total energy: TE + = CE[i]

Total energy is calculated by overall Consumed Energy (CE)

Average energy: AE = TE / n

Total energy is calculated by using Total energy divided by Number of nodes.

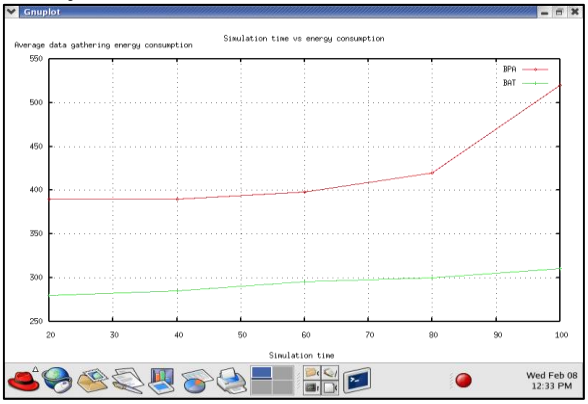


Fig. 5: Total energy

VI. CONCLUSION

Our proposed hierarchical clustering structure provides secure transmission. Threshold value which provides better pairs which doesn't give chance for the attacker to hack the packet information. We achieve high throughput and delay tolerant mechanism via simulation results. The proposed framework is PKI-compatible and is ready to be integrated with existent PKI enhancements. Particularly, for real-world adoption of the proposed techniques, a certificate user should well protect her secret keys and never disclose any certificate before activation. Otherwise, the user risks losing all the security benefits of our frame-work may offer. We suggest that any public/private key pair (and hash key for ADC, if any) yet to be used be kept in physically secure storage, which means a certificate correlation tree (or chain) should never be built on an online platform. Accordingly, the CA may need to educate a user to be meticulous and responsible, and provide a specialized user device to facilitate her key management, as our framework of generating correlated certificates is trans-parent to the CA but the overhead is shifted to the user side.

REFERENCES

[1] Lein Harn and Jian Ren, Generalized Digital Certificate for user authentication and key establishment for secure communications IEEE transactions on wireless communications, vol. 10, no. 7, july 2011.

[2] Ji Young Chun, Jung Yeon Hwang, and Dong Hoon Lee, a note on leakage-resilient authenticated key exchange IEEE transactions on wireless communications, vol. 8, no. 5, may 2009.

[3] D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, document RFC 5280, May 2008.

[4] J. Clark and P. C. van Oorschot, "SoK: SSL and HTTPS: Revisiting past challenges and evaluating certifi cate trust model enhancements," in Proc. IEEE SP, May 2013, pp. 511–525.

[5] J. Lin, W.-T. Zhu, Q. Wang, N. Zhang, J. Jing, and N. Gao, "RIKE + : Using revocable identities to support key escrow in public key infrastrucures with flexibility," IET Inf. Secur. , vol. 9, no. 2, pp. 136–147, Mar. 2015.

[6] T. Kleinjung et al., "Factorization of a 768-bit RSA modulus," in Proc. CRYPTO , Aug. 2010, pp. 333–350.

[7] N. Leavitt, "Internet security unde r attack: The undermining of digital certificates," Computer , vol. 44, no. 12, pp. 17–20, Dec. 2011.

[8] A. K. Lenstra, "Generating RSA moduli with a predetermined portion," in Proc. ASIACRYPT, Oct. 1998, pp. 1–10.

[9] M. Joye, "RSA moduli with a predetermined portion: Techniques and applications," in Proc. ISPEC, Aug. 2008, pp. 116–130.

[10] Wen Tao Zhu and Jingquiang Lin, Generating Correlated Digital Certificates: Framework and Applications", vol .11, No. 6 June 2016.

[11] Eastlake D and Hansen T, US Secure Hash Algorithms (SHA and SHA Based HMAC and HKDF), document RFC 6234, May 2011. ZHU AND LIN: Generating Correlated Digital Certificates 1127.

[12] Gañán C, Mata-Díaz J, Mu noz J L, Hernández-Serrano J, Esparza O, and Alins J, "A modeling of certificate revocation and its application to synthesis of revocation traces," IEEE Trans. Inf. Forensics Security, vol. 7, no. 6, pp. 1673–1686, Dec. 2012.
[13] Harn L and Ren J, "Generalized digital certificate for user authentication and key establishment for secure communications," IEEE Trans. Wireless Commun., vol. 10, no. 7, pp. 2372–2379, Jul. 2011.
[14] Ji Young Chun, Jung Yeon Hwang and Dong Hoon Lee, A Note on Leakage- Resilient Authenticated Key Exchange, IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 8, NO. 5, MAY 2009.
[15] Jonsson J and Kaliski B, Public-Key Cryptography Standards (PKCS) #1: RSA Cryptography Specifications Version 2.1, document RFC 3447, Feb. 2003.
[16] D.Chaum and H. van Antwerpan, "Undeniable signatures", Advances in cryptology – crypto- 89, Lecture Notes in Computer Science, vol. 435, pp. 212-217, 1989.
[17] Kitahara M, Yasuda T, Nishide T, and Sakurai K, "Upper bound of the length of information embed in RSA public key efficiently," in Proc. Asia PKC, May 2013, pp. 33–38.
[18] Kleinjung T et al., "Factorization of a 768-bit RSA modulus," in Proc. CRYPTO, Aug. 2010, pp. 333–350.
[19] Kleinjung T, Bos J W, and Lenstra A K, "Mersenne factorization factory," in Proc. ASIACRYPT, Dec. 2014, pp. 358–377.
[20] M. Jakobsson, K. Sako, and R. Impagliazzo, "Designated verifier proofs and their applications," Advances in Cryptology -EUROCRYPT, pp. 143-154, 1996. LNCS Vol 1070.
[21] Laih C S and Chen K Y, "Generating visible RSA public keys for PKI," Int. J. Inf. Secur., vol. 2, no. 2, pp. 103–109, Jan. 2004.
[22] Laurie B, "Certificate transparency," ACM Queue, vol. 12, no. 8, p. 10, Aug. 2014.
[23] Ryan M D, "Enhanced certificate transparency and end-to-end encrypted mail," in Proc. NDSS, Feb. 2014, pp. 1–14.
[24] Devisree U, Santhi M, Efficient Cluster Based CCRVC Scheme in Manet, International Journal of Innovative Research in Computer and Communication Engineering, ISSN (Online): 2320-9801.

