International Journal of Engineering Research and Technology. ISSN 0974-3154, Volume 13, Number 12 (2020), pp. 4701-4705
© International Research Publication House. http://www.irphouse.com

Efficient Identity-Based Batch Signature Scheme to Reduce Energy Consumption at Mobile Receivers

Jagadeesha R[1] and Thippeswamy K[2]

[1]*Department of Computer Science & Engineering, Kalpataru Institute of Technology,
Hassan Circle, Tiptur-572201, VTU, Belagavi India.*

[2]*Department of Studies in Computer Science and Engineering VTU Center for PG-Studies,
Regional Office, Ring Road, Hanchya Sathagally Layout, Mysore-570019, Karnataka, India.*

Abstract

Identity-based signature authentication (IBSA) scheme for delay-tolerant sensor networks using online/offline signature batch authentication reduces the computation cost and improves efficiency in the delivery of packets. However, the energy of the mobile sensor network or mobile node in a multicast network is a critical issue to be addressed clearly. In our proposed modified IBSA scheme smallest least unused random number is selected for master secret, using this master secret public secret is derived. The computation cost for batch signature generation and verification is minimized in a multicast network with both static and mobile nodes, which impacts on processing time of batch signature verification. Processing time and energy required for batch signature verification is less when compared to existing schemes. Processing time required for signature verification is linearly proportional to the energy of the node in a network. Mobile node battery source has a finite lifetime. Energy at the mobile node is the key parameter to increase the lifetime of a mobile node. The processing cycle required for batch verification is recorded by the receiver periodically to compare the energy consumption by the mobile node at different time intervals.

Keywords: Energy, Multicast, Mobile Receiver, Signature verification.

1. INTRODUCTION

In recent days due to the rapid use of the internet for different applications: stock exchange, online video game, and video conferencing, etc., Information transfer from a single sender to multiple receivers is usual communication mode in computer networks which was not popular in early days of the internet. The receiver has to verify whether data has come from the intended sender and whether the data has been altered or not during transit. The problem is if intruder [01] forwards forged data to the receiver then the receiver has to spend more time to verify than unforged data which is a burden to the receiver having low processing capability. Authentication can be carried out using symmetric key cryptography [02] but both encryption and decryption are carried out using the same secret. So the probability of forging data and hacking the key is more in symmetric key cryptography when compared to asymmetric key cryptography. Intruder can act as a real member node in a multicast network if he gets a key. So it's not recommendable to all the critical multicast application [03]. Authentication using asymmetric key cryptography [02] uses separate keys for both encryption and decryption. Source node uses a public key to encrypt data and the recipient uses a private key to decrypt data which is known only to the receiver. Symmetric key cryptography is used in some of the applications where a large amount of data to be transferred and creates less processing overhead to nodes in a network but when coming to security services asymmetric key cryptography is the best choice even though it creates more overheard to nodes in a network.

Digital signature is a asymmetric key cryptography, the best authentication scheme for most of the multicast applications. Digital signature algorithms require more computation, each packet is signed and verified independently [04] [05], not the best choice for resource-constrained devices. Schemes in [06] [07] uses one signature for a block of packets computation cost is minimized when compared to a per-packet signature. Scheme in [08] authenticates many packets simultaneously with verification of one signature. Day by day mobile devices are becoming the most dependable thing to people for their different purposes. The efficient utilization of resources is given paramount importance in mobile devices [09] and authentication is also considered without compromising security services and reducing the overhead at the mobile receiver to a maximum level. Some of the multicast applications aim at the delivery of information to the recipient with acceptable minimum delay experienced in the network. Delay should not impact on the satisfaction of the users, sometimes which leads to termination of service. Previous research on multicast authentication using batch signature [08] schemes and identity-based signature scheme [10] minimizes computation cost to the minimum extent best suitable for static receivers but not for mobile receivers (which have limited processing capability). Computation cost is to be minimized to the maximum level for mobile receivers in a multicast network [11].

In this paper, authentication is carried out using asymmetric key cryptography (digital signature) by considering the energy and resource of multicast mobile receiver. In a multicast network source node is a static node forwards messages to all the nodes in a network, the receiver node may be static or mobile. Source node collects information of all the nodes in the network, all nodes in the network collects information about their neighbour for routing and exchange information. Here we are using motive state-based data delivery scheme [12] where all nodes in the network sends request to source node and get secure identity, consumes more energy and resources. A separate modified scheme is required for resource-constrained mobile receivers in a multicast network. The processing cycle required for task completion is to be considered while designing a methodology for energy constraint mobile receivers. Generally energy of a device is calculated by the power utilized during the processing and idle state. The power utilized by the device during the idle state is negligible when compared to power utilized in processing an application. Our research paper is organized as follows: part 1: focused on the introduction part 2: related works and drawbacks. Part 3: Research method. Part 4: compares the results and findings of research carried out. Part 5: highlights the conclusion of the proposed work.

2. RELATED WORK

The online/offline signature scheme [13] is suitable for resource-constrained devices like mobile phones. In [13] signature generation is divided into two different phases: i) online and ii) offline. Offline phase (message is not known) applied when there is too much computation needed. Online phase (message is known) is applied when there is less computation needed. IBC based online/offline signature scheme (IBSOO) [14] are well suitable method for wireless node, which minimizes processing time for online/offline signature in real-time applications. Switching from online to offline and vice-versa itself creates overhead to the receiver due to limited resources available for processing. Delay occurred in processing and display of contents must tolerate to some extent. Scheme [15] is suited for delay tolerant networks but it has high processing overhead not suitable for mobile receivers.

In multicast routing nodes forwards 'n' number of copies of data, so data to be stored on the node depends on the memory space of the message queue or buffer. In most of the routing schemes, nodes will not receive messages or data until the memory is available to hold new incoming messages. If the message arrived at the node is not received, it will be discarded after timeout [16]. Loss of data due to the message queue at the node can be overcome by applying the computation efficient type-1 method. But message queue is not able to process or store batch messages even by type-1 [16] are not addressed. So scheme should address loss of data due to message queue full and should be computationally efficient in authenticating batches. In this paper, we are not considering time delay occurred in the intermediate node for signed batch transmission and line rate. We are considering only the energy and processing time after the arrival of signed batches to the receiver. We are using (MSAD) [12] scheme routing scheme for transferring signed batches from the sender to all the destinations in the multicast network.

Energy efficiency in mobile devices is increased in [17], increasing the battery capacity and extending circuit board physical space which may be effective in small message transmission or simple network but not suitable for multicast real-time applications where processing of application will be done in milliseconds. Scheme in [17] uses upgrading battery capacity dynamically itself creates overhead to receiver and takes multiple interaction messages. Scheme in [18] uses near-optimal solutions for placing sensor nodes in a network, to maximize the node lifetime distribution model is used. Sensor nodes communicate with each other and distribute energy consumption with each other. But in real-time multicast applications, difficult to exchange information between neighbours when application running is in progress, even if the communication is taken place during execution, which consumes more processing cycles and increases the time required to complete the execution of the application. The distribution model may increase the lifetime of the sensor node but it uses extra resources and time of the mobile node so not suitable for mobile node with limited resource and processing capability. Our objective is to efficient utilization of energy at the mobile receiver during signature verification.

3. PROPOSED METHODOLOGY

Identity –based signature batch authentication is used for signature generation and verification. Energy utilized by receiver's to verify batch signature is calculated based on the processor utilization time at that time.

3.1 Improved identity-based signature batch authentication

Unlike [16] we consider one sender and multiple receivers (multicast network), key generator function to generate system parameter, and secret key. Key generator function is present at the source node N_s and $N_{1,}$ $N_{2,}$ $N_{3,}$ N_4 ………$N_{n.}$ are remaining nodes in a multicast network. Before the start of message transmission sender source node generates bilinear parameters (p, P,g1,g2,ê), ê is non-degenerated

Two common cryptographic hash functions are used in all the nodes in the multicast network

$$H_x:\{0,1\} \rightarrow Kp, \quad (1)$$

$$H_{y:}:\{0,1\}.\ g\ .\ g2 \rightarrow Kp \quad (2)$$

Source node generates random number α, α∈ Kp which is a master secret key Scheme [16] chose a random number, if we consider a large random number it creates unnecessary overhead to the nodes and requires high computation, so in our scheme, we consider a small random number which is not used in recent message transmission as α

By using the master key α, the source node calculates public key Pb ⟵ αP

Source node transmits the system parameters and the secret key to any network node upon request.

$$Sn = P/(Hx(N))+ \alpha \quad (3)$$

3.1.1 Signature generation

Consider message Ms to be signed by private key at the source node in a network.

Choose a small random number' b' which is not used in recent message transmission, b∈Kp and compute b^{-1} than choose another random number u∈Kp and compute $R = ê(p,P)^{u}$, Ss = bSn and computes $\sigma = (R,u, b^{-1}Ss)$. (4)

Now compute

h = Hy(Ms,R,Ss), (5)

$\theta = (u+h).\ b^{-1} \mathrm{mod}\ p$ (6)

$\sigma = (N, R, \theta, Ss)$ (7)

3.1.2 Signature verification

h= (Hy(Ms,R,Ss) (8)

if $Rê(p,P)^{h} = ê(\theta,Ss,Hx(N)P+Pb)$ (9)

than signature is verified successfully.

3.1.3 Batch Signature verification

In batch signature multiple signatures are verified simultaneously in our scheme computation cost is less when compared to [16], we considered unused small random number for key generation. Scheme in [16] applied multiple intermediate nodes as they receive messages from multiple sources. In our scheme, we considered only a single sender and multiple receivers. When messages from the sender is signed and transferred, the signature of batches are verified by following

$R_{batch} = \prod_{j=1}^{i} Ri$ (10)

$\Theta_{batch} = \sum_{j=1}^{i} \Theta i$ (11)

$h_{batch} = \sum_{j=1}^{i} hi$ (12)

If $R_{batch}ê(P,P)^{hbatch} = ê(\theta_{batch}, Ss,Hx(N)P+Pb)$ (13)

than batch verified, otherwise batch is not verified.

3.2 Energy consumption calculation during Signature verification

The total time taken by the processor to complete the batch signature verification is linearly proportional to the energy utilized by the node. If the energy at a particular stage is reached to low or the buffer to hold bathes is not capable of holding incoming batches then the sender is informed to stop transmission until a further request from the receiver leads to data play out with tolerable delay but reduces loss of data. 'Ts' is the size of the buffer 'B' to hold incoming packets at the mobile node. 'As' is the available space in the buffer 'B' to hold the incoming packets at the node. When signed batches arrive at the mobile node, the mobile node checks whether the available buffer space is sufficient to hold the incoming packets.

As = $\sum_{i=1}^{n} f(x)$ (14)

F(x) = Check(B) (15)

'**E_{total}**' is the total energy utilized by the node, '**E_{idle}**' is the energy utilized before the start of signature verification and '**E_{active}**' is the energy utilized during batch signature verification. Generally, energy utilized by the node depends on the battery power consumed to process the application. Here energy utilized by the mobile node is calculated by the amount of power utilized at the mobile node for batch signature verification.

$E_{total}= E_{idle}+ E_{active}$ (16)

The energy consumption of receiving node receiving 'Y' batches of m bit data each is 'E(Y)'. 'E_{unit}' is the amount of energy consumed for the processing unit of data bit. 'E_{unit}' is calculated by the processing of 100 batches, each batch with 10 packets of 1024 bytes.

$E(Y) = Y * m * E_{unit}$ (17)

4. PERFORMANCE EVALUATION

In our proposed improved IBSA for mobile receivers, processor utilization for signature verification is calculated to check for energy consumed by the mobile receiver.

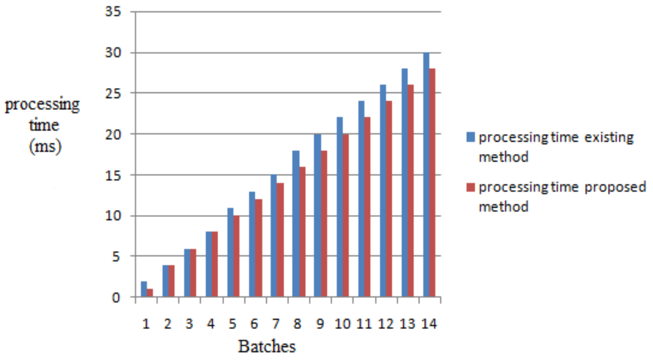

Figure I. Number of batches processed over time

Fig. I shows the number of batches processed (signature is processed) by the processor over time. We evaluated both existing and proposed methodology for batch signature verification by the processor and the time taken to verify batches. Here time is measured in milliseconds, one processing cycle or processing unit is equal to one millisecond. One batch unit in the graph is equal to ten batches, 1 batch contains ten packets. At batch unit 1 processing time is two milliseconds in the existing method. At batch unit two, three, and four processing time in our existing method and proposed is the same. In certain situations processing time at the node is varied due to the size of the key or the processor delay, so in some batch signature verification processing time in both existing and proposed methods is the same. For this reason, we have evaluated the processing time batch unit's signature verification from one to fourteen. We have considered the average processing time is taken in batch unit signature verification than our proposed method takes approximately 30% less processing time to verify batch signature when compared with the existing method.

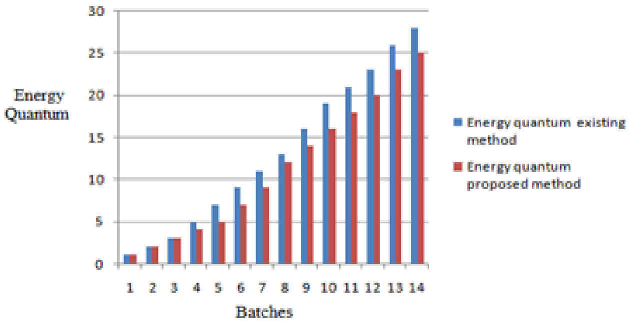

Figure II. Energy quantum verses batches

Fig II. Shows energy quantum utilized to process batches, one batch unit is equal to ten batches, and each batch contains ten packets. One energy quantum we considered as one millijoule Energy quantum utilized by the processor in existing and proposed method at batch units 1,2,3 is the same it's due to key size chosen or processor delay. From the batch unit from four to fourteen average quantum of energy utilized by the processor based on the processing time utilization is almost 50% less when compared with the existing method for signature verification.

5. CONCLUSION

Results show the proposed method in this paper utilizes less energy quantum when compared to the IBSA scheme. Computation cost during the signature processing is also minimized. Processing time needed to verify the batch signature is also minimized. Loss of data due to buffer full is also addressed. The proposed method is well suited for mobile receivers in a multicast network which has low processing capability.

REFERENCES

[1]. H. Azwar, M. Murtaz, M. Siddique, "Intrusion Detection in secure network for Cybersecurity systems using Machine Learning and Data Mining," 2018 IEEE 5th International Conference on Engineering Technologies and Applied Sciences (ICETAS), S. Rehman et al., Bangkok, Thailand, 2018, pp. 1-9, doi: 10.1109/ICETAS.2018.8629197.

[2]. M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," 2017 International Conference on Engineering and Technology (ICET), Y. Khamayseh et al., Antalya, 2017, pp. 1-7, doi: 10.1109/ICEngTechnol.2017.8308215.

[3]. G. Araniti, M. Condoluci, P. Scopelliti, A. Molinaro, "Multicasting over Emerging 5G Networks: Challenges and Perspectives," in IEEE Network, A. Iera et al., vol. 31, no. 2, pp. 80-89, March/April 2017, doi: 10.1109/MNET.2017.1600067NM.

[4]. S. Even, O. Goldreich, and S. Micali, "On-Line/Offline Digital Signatures," J. Cryptology, vol. 9, pp. 35-67, 1996.

[5]. P. Rohatgi, "A Compact and Fast Hybrid Signature Scheme for Multicast Packet," Proc. Sixth ACM Conf. Computer and Comm. Security (CCS '99), Nov. 1999.

[6]. C.K. Wong and S.S. Lam, "Digital Signatures for Flows and Multicasts," Proc. Sixth Int'l Conf. Network Protocols (ICNP '98), pp. 198-209, Oct. 1998.

[7]. C.K. Wong and S.S. Lam, "Digital Signatures for Flows and Multicasts," IEEE/ACM Trans. Networking, vol. 7, no. 4, pp. 502- 513, Aug. 1999.

[8]. Y. Zhou, X. Zhu, and Y. Fang, "MABS: Multicast Authentication Basedon Batch Signature," IEEE Transactions on Mobile Computing, vol. 9, no. 7, pp. 982-993, July 2010.

[9]. Salman, M.K. & Ahmad, R.Badlishah. (2014). A new approach for efficient utilization of resources in WiMAX cellular networks. Yahya, Abid et al., Tehnicki Vjesnik. 21. 1385-1393.

[10]. C. Zhang, R. Lu, X. Lin, P. -. Ho and X. Shen, "An Efficient Identity-Based Batch Verification Scheme for Vehicular Sensor Networks," *IEEE INFOCOM 2008 - The 27th Conference on Computer Communications*, Phoenix, AZ, 2008, pp. 246-250, doi: 10.1109/INFOCOM.2008.58.

[11]. Wang, L., Gao, S., Zhang, H. *et al.* Mobile multicast source support in PMIPv6 networks. *J Wireless Com Network* **2013,** 152 (2013). https://doi.org/10.1186/1687-1499-2013-152

[12]. Li W J, Zheng K F, Zhang D M, et al. Motive state-based data delivery scheme of delay tolerant mobile sensor network. Journal of Nanjing University of Science and Technology, 2012, 36(9): 150156 (in Chinese).

[13]. Radhika, K.S. & Saju, Gopika. (2015). Online and Offline Signature Verification: A Combined Approach. Procedia Computer Science. 46. 1593-1600. 10.1016/j.procs.2015.02.089.

[14]. Ming Y, Wang Y M. Improved identity based online/offline signature scheme. Proceedings of the 7th International Conference on Autonomic and Trusted Computing (UIC/ATC'10), Oct 26-29, 2010, Xi'an, China. Piscataway, NJ, USA: IEEE, 2010: 126-131.

[15]. Zhu H J, Lu R X, Shen X M, et al. BBA: an efficient batch bundle authentication scheme for delay tolerant networks. Proceedings of the IEEE Global Telecommunications Conference (GLOBECOM'08), Nov 30-Dec 4, 2008, New Orleans, LA, USA. Piscataway, NJ, USA: IEEE, 2008: 5p.

[16]. Wen-ji LI, Kang-feng ZHENG, Dong-mei ZHANG,

Qing YE,Efficient identity-based signature scheme with batch authentication for delay tolerant mobile sensor network,The Journal of China Universities of Posts and Telecommunications, Yi-xian YANG et al., Volume 20, Issue 4, 2013, Pages 80-86, ISSN 1005-8885.

[17]. G. Bhatia, R. Mahajan and S. K. Khatri, "A study for improving energy efficiency in mobile devices," 2017 International Conference on Infocom Technologies and Unmanned Systems (Trends and Future Directions) (ICTUS), Dubai, 2017, pp. 588-592, doi: 10.1109/ICTUS.2017.8286077.

[18]. Dutta, Raju & Gupta, Shishir & Das,. (2012). Power Consumption and Maximizing Network Lifetime During Communication of Sensor Node in WSN. Procedia Technology. Mukul et al., 4. 158–162. 10.1016/j.protcy.2012.05.023.

BIOGRAPHIES OF AUTHORS

	Mr. Jagadeesha R Currently working as Asst.Professor in Department of CSE at Kalpataru Institute of Technology, pursuing Ph.D degree in Computer Science and Engineering from VTU, Belagavi, Karnataka, India.
	Dr. K. Thippeswamy. Currently working as **Professor & Program coordinator** Department of Studies in Computer Science and Engineering VTU Center for PG-Studies, Regional Office, Mysore, Karnataka, India. His research interest includes Computer networks, Data Mining & Cloud Computing.