Authenticating with Privacy Protection in Opportunistic Networks

Ming-Huang Guo
Department of Information Management,
Shin-Hsin University
Email: mhguo@mail.shu.edu.tw

Horng-Twu Liaw
Department of Information Management,
Shin-Hsin University
Email: htliaw@cc.shu.edu.tw

Meng-Yu Chiu
Department of Information Management,
Shin-Hsin University
Email: cmy@cc.shu.edu.tw

Li-Ping Tsai
Department of Information Management,
Shin-Hsin University
Email: cute08312002@hotmail.com

***Abstract*—In this study, we propose an authentication mechanism with privacy protection for opportunistic networks. It is applied for the short-term and limited-time wireless network environment, and a super node is set to manage node registration. The proposal implements some encryption and security technologies to against security threats and attacks. In the analysis, the proposed mechanism finishes the authentication with less data, and provides anonymity and user privacy in the network.**

Keywords: Opportunistic Network, Privacy Protection, Authentication Mechanisms.

I. Introduction

An opportunistic network (OppNet) is a type of delay-tolerant network that is composed of mobile and super nodes. An OppNet comprises the following features: In an OppNet environment, nodes are intermittently connected; there are no permanent source–destination end-to-end paths between nodes; disconnections and reconnections frequently occur between nodes; and the network connectivity is highly variable.

In an OppNet, all network topologies are variable. Adequate path-planning strategies must be implemented to prevent data loss and reduce interference. Moreover, node mobility enables OppNet to be applied in crisis management [2], [7]. During data transmission, OppNets are connected through user device when the user is moving, thus completing message transmission. However, this transmission method is accompanied by the security problem of uncertainty during movements. For example, users may not be aware of whether randomly encountered nodes are secure and may be attacked when they encounter malicious nodes [8], [9]. In addition, protecting users' personal privacy is another crucial concern. OppNet-related studies have mostly emphasized designing resource-efficient routing methods and have seldom focused on the protection of personal data and privacy. Therefore, the present study proposes an OppNet-specific authentication scheme for preventing malicious node attacks and protecting personal privacy.

II. Related Works

Poonguzharselvi et al. [1] proposed using trust value thresholds for selecting nodes and providing transmission services. Trust values between neighboring nodes are similar to trust levels between people. When transmitting data, a node individually calculates the trust values between itself and the remaining nodes to eliminate malicious nodes and increase the security of data transmission.

Goyal et al. [3] proposed placing seed nodes in OppNet environments to provide general node registration and store data. When source nodes connect to destination nodes, the connectivity must be reported by connecting to the seed node; moreover, virtual identifications (IDs) are transmitted from seed nodes to source nodes to obtain transmitted data from destination nodes. Furthermore, super nodes are used for managing user data and applying public and private key encryption techniques to general nodes to ensure data security.

Ren et al. [6] proposed a source anonymous message authentication scheme, which can anonymize destination node IDs, enable data transmission from source codes, prevent attackers from calculating destination nodes through tapping and tracing packet transmission paths, increase the security of data transmission, and protect destination IDs.

By using mobile devices and household and external proxies, Kuo et al. [10] proposed a registration and authentication scheme for ameliorating the challenges faced in controlling IDs in mobile devices, thereby providing protection against various forms of attacks.

III. Proposed Scheme

Figure 1 illustrates the network environment of the proposed scheme; each node is described subsequently.

1) *Super Nodes:* These are immobile nodes that are set within OppNets. When new nodes enter the network, they must register at the super nodes and obtain authentication credentials. When nodes require security confirmation, they may use the super nodes for verification.

2) *Authenticated Nodes:* These are nodes that have been authenticated by the super nodes and may represent users' mobile devices or equipment, such as tablets and laptop computers.

3) *Unauthenticated Nodes:* These are nodes that have not yet completed registration with the super nodes, their IDs are thus unknown.

QSHINE 2015, August 19-20, Taipei, Taiwan

DOI 10.4108/eai.19-8-2015.2260862

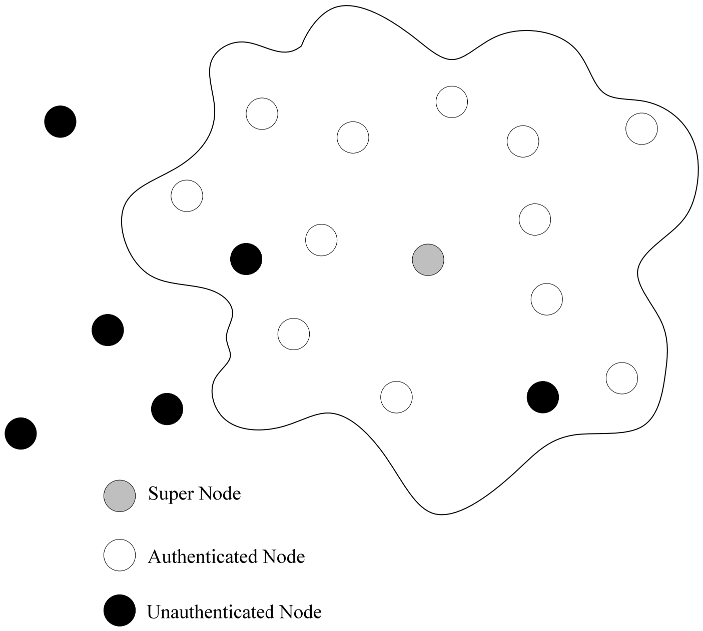

Figure. 1. Network environment.

TABLE I. SYMBOLS

Symbol	Description
ID_i	virtual ID of node *i*
PK_i	public key of node *i*
SK_i	private key of node *i*
E_{key}(m)	key encrypted message *m*
D_{key}(m)	key decrypted message *m*
h( )	hash operation
M_j	authentication credentials from the super node at time j; this credential is periodically updated (i.e., every 4 or 6 h)
f( )	arithmetic function in the session key that is generated by the super node for the general node
T_i	timestamp for the connection between node *i* and other nodes
K_{sn}	symmetric-key of the super node; this is updated hourly
$SessK_{iu}$	session key for node *i* and node *u*
$A \oplus B$	XOR operation between *A* and *B*

A. *Assumptions*

The following assumptions were thus developed in this study:

1) Each user’s mobile device that enters the network is considered an individual node. Each device possesses basic computation and storage abilities.

2) The OppNet adopts the local area network technology. Mobile network connections (i.e., 3G) are not discussed and secure channels are absent.

3) The mutual authentication and privacy protection of nodes were strictly emphasized and authenticated data transmission was excluded.

4) The OppNet refers to temporary gathering occasions. User registrations are processed at a service counter; super nodes are set at the service counter and nodes register at super nodes when they enter the area of proximity (less than 1 m).

5) Super nodes provide only authentication assistance, which excludes network message transmission, network topology, or transmission paths.

This study categorized the privacy types in the OppNet as user privacy and device privacy according to the privacy descriptions provided in related studies [4], [5]. Table I lists the symbols used in this study.

B. *Registration and Authentication Phases*

In the network environment depicted in Figure 1, the nodes are registered and authenticated at the super node when entering the network area. Therefore, the procedures in this study were divided into two stages, which are the registration process and authentication process. These processes are described in the following subsections.

1) Registration Process: In this process, nodes register at the super node when they enter the network. Consider, for example, Node A; Figure 2 illustrates the procedures at the registration stage.

a) Node A requests registration from the super node. When users register at the service counter with their handheld devices, a super node device is provided at the service counter for registration services.

b) The super node responds to the request and transmits PK_{sn}.

c) When Node A receives the response, it calculates $h(ID_a)$.

d) Node A uses PK_{sn} to encrypt PK_a and returns $h(ID_a)$ to the super node.

e) When the super node receives the packet, a private key is used to unlock the packet, obtain and store PK_a and $h(ID_a)$, and generate M_j and T_{sn}.

f) Subsequently, the super node uses the PK_a encryption provided by Node A; this encryption comprises M_j, the XOR value of $h(ID_a)$, operation function $f(\ )$ of Node A, K_{sn}, and T_{sn}. These data are then encrypted and returned to Node A. At this moment, the XOR operation provides authentication for only Node A to prevent risks of data leakage.

g) When Node A receives the data, it operates using a private key and its own ID and obtains and stores M_j, $f(\ )$, and K_{sn} provided by the super node.

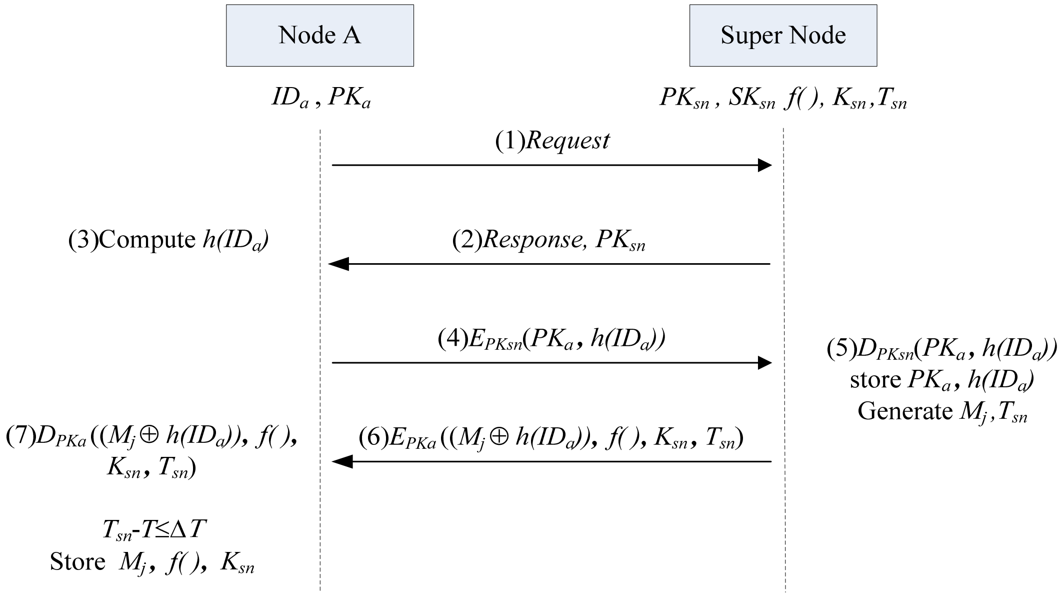
Node A
Super Node
ID_a , PK_a
PK_{sn} , SK_{sn} $f(\ )$, K_{sn} ,T_{sn}
(1)*Request*
(3)Compute $h(ID_a)$
(2)*Response*, PK_{sn}
(4)$E_{PKsn}(PK_a, h(ID_a))$
(5)$D_{PKsn}(PK_a, h(ID_a))$
store PK_a, $h(ID_a)$
Generate M_j ,T_{sn}
(7)$D_{PKa}((M_j \oplus h(ID_a)), f(\ ),$
$K_{sn}, T_{sn})$
(6)$E_{PKa}((M_j \oplus h(ID_a)), f(\ ), K_{sn}, T_{sn})$
T_{sn}-$T \leq \Delta T$
Store M_j, $f(\ )$, K_{sn}

Figure 2. Registration process.

2) Authentication Process: When Node A completes the registration process, it moves within the environment. Assume Node A seeks to transmit data to Node B; Node A may authenticate the ID of Node B and confirm whether Node B has completed the registration process at the super node. Figure 3 shows the authentication process, the procedures of which are elaborated as follows:

a) First, Node *A* performs a hash operation on M_j and generates T_a.

b) PK_a, $h(ID_a)$, and XOR values of M_j, M_j, and $h(M_j)$ in addition to $h(ID_a)$ and T_a are encapsulated and encrypted using the symmetric key of the super node and returned to Node *B*.

c) When Node *B* receives the packet, it unlocks it by using the symmetric key of the super node to extract the contents. At this moment, Node *B* computes its own authentication credential M_j' and the XOR value of $h(M_j')$. If the XOR value of M_j and $h(M_j)$ are equal, then the authentication credentials for both parties are provided by the super node and that $h(M_j')$ and $h(M_j)$ are equal; therefore ID_a and T_a can be solved. If the aforementioned XOR values are different, the connection terminates.

d) T_a and packet arrival time T are subtracted to obtain ΔT to verify whether ΔT is within the normal transmission period and to terminate expired connections. If the connection remains valid, $h(ID_a)$ and T_a of Node A and ID_b, M_j', and T_b of Node *B* are substituted into the arithmetic function *f( )* to compute $SessK_{ab}$'.

e) Next, $h(ID_b)$ of Node *B* as well as the XOR computed values of M_j', M_j', and $h(M_j')$, and $h(ID_b)$ and T_b are encapsulated using PK_a encryption and returned to Node *A*.

f) As Node *A* receives this packet, it uses SK_a to unlock the packet and extract the contents. At this moment, Node *A* confirms if the XOR values of M_j and $h(M_j)$ are equal to those of M_j' and $h(M_j$'). If these values are equal, Node *A* obtains the contents and $h(ID_b)$, M_j', $h(M_j')$, and T_b of Node *B*; otherwise, the connection is terminated.

g) Node *A* confirms T_b and whether ΔT' (difference between T_b and Node *A's* packet arrival time *T)* falls within the normal transmission period. If ΔT' does not fall within the aforementioned range, the connection terminates; otherwise, $h(ID_a)$ and T_a of Node *A* and $h(ID_b)$, M_j, and T_b of Node *B* are substituted into *f( )* to calculate $SessK_{ab}$.

h) Node *A* uses $SessK_{ab}$ to encrypt the connection request.

i) Node *B* uses $SessK_{ab}$' for the decryption; the session keys computed by the two nodes are equal if the encrypted messages can be unlocked.

j) If the session keys vary, the connection terminates; otherwise, $SessK_{ab}$' is used to encrypt the returned connection reply.

k) Node *A* uses $SessK_{ab}$ to encrypt the connection request and connection reply. The session keys computed by both nodes are equal if these encrypted messages can be unlocked. Subsequently, data transmission may proceed between Nodes *A* and *B.*

The mutual authentication and node ID confirmation between users are completed in the aforementioned process. After this process, nodes may perform data transmission or trust evaluation (in combination with other studies). The proposed scheme for the authentication, privacy protection, and data transmission between nodes in OppNets is thus demonstrated in the aforementioned method.

IV. Security Analysis

In the following discussion, privacy protection in OppNets and prevention against various security threats are analyzed.

A. Privacy Protection

Regarding users' privacy protection, PK_a and $h(ID_a)$ of Node A are transmitted when Node A registers at the super node (Step 4, Fig. 2). During this process, the data stored in the super node are processed hash values, and plaintexts are not kept; therefore, this protects the super node from privacy leakage. In addition, super nodes strictly provide node registration within networks; network topology is not maintained. Therefore, user and node mobility are not recorded and their trajectories not traced, thereby eliminating any concern regarding location privacy. In addition to the IDs of hashed node devices, the data used in this study did not contain other user and device data, reducing the use of user data and indirectly preventing data leakage. Moreover, during each authentication transmission, the data packet for the authentication between each pair of nodes contained *T*s and updated *M*s. Therefore, each authentication uses different data, excluding equipment data. This prevents intentionally collecting node data and exposing node traces and improves the transmission privacy of users and privacy of mobile network equipment.

B. Tapping Attack

In the network environment, malicious attackers can tap and collect data, such as messages transmitted between devices and the super node during authentication processes. To prevent these processes, asymmetric public key encryption was used before message transmissions in the proposed scheme (Step 2, Fig. 3). Although malicious attackers can tap the transmitted messages when users use devices to register at the super node, the signals are encrypted ciphertexts; malicious attackers must have decryption keys to obtain the messages. Therefore, tapping attacks can be prevented in the proposed scheme.

C. Forgery Attack

There are two types: component heads and text heads. Forgery attack is a technique used by malicious attackers to disguise as legitimate devices. Protections are provided when authenticating node IDs through hashing device IDs and *M*s. During transmission processes, the XOR values of *H(ID)* and *H(M)* are transmitted; consequently, attackers may not individually steal any data item for forging IDs. Because transmission data and IDs are computed together, individual data cannot be unlocked. This confirms the hourly update of *M* and prevents repeated usage. Furthermore, although secure channels are absent during registration, nodes provide strictly their own public keys and ID hash values. Malicious nodes that present intentions to forge the super node and bait node data may obtain only the public keys and ID hash values, but are prevented from accessing other corresponding data to unlock packets. Therefore, the proposed scheme can prevent forgery attacks.

D. Resend Attack

In this scheme, *T*s are generated when messages are transmitted between nodes (Step 1, Fig. 3). User requests are declined when the node identifies expired timestamps. Therefore, attackers cannot repeatedly tap transmission messages and perform resend attacks.

E. Man-in-the-middle Attack

In this attack technique, *T*s are also added during message transmissions; moreover, asymmetric encryption is adopted. Because cracking is time-consuming in this scheme, message transmissions expire when attackers attempt to crack and tamper with message contents. Therefore, tampered messages cannot pass node authentication processes.

F. Anonymity

In this scheme, hashed IDs are used during node authentication; therefore, nodes cannot obtain the true IDs of other nodes to capture relevant device or user's privacy data. The XOR values of H(ID) and H(M) are adopted during message transmission and the symmetric key of the super node is used to encrypt transmissions. Consequently, malicious nodes cannot access the original message contents. The IDs of these nodes are immune to tracing; the connection records are also resistant to leakage. Therefore, the proposed scheme ensures the privacy of device and user data and the security of data transmission and storage.

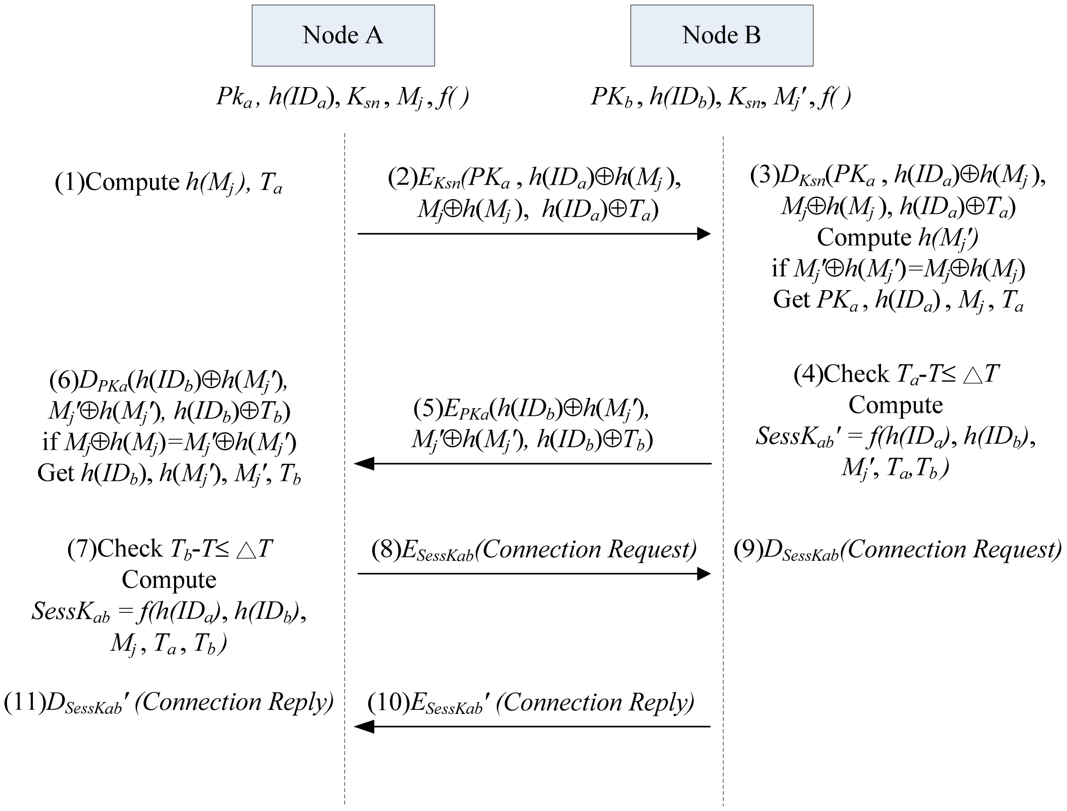
Node A
Node B
Pk_a, $h(ID_a)$, K_{sn}, M_j, $f(\,)$
PK_b, $h(ID_b)$, K_{sn}, M_j', $f(\,)$
(1)Compute $h(M_j)$, T_a
(2)$E_{Ksn}(PK_a, h(ID_a)\oplus h(M_j), M_j\oplus h(M_j), h(ID_a)\oplus T_a)$
(3)$D_{Ksn}(PK_a, h(ID_a)\oplus h(M_j), M_j\oplus h(M_j), h(ID_a)\oplus T_a)$
Compute $h(M_j')$
if $M_j'\oplus h(M_j')=M_j\oplus h(M_j)$
Get PK_a, $h(ID_a)$, M_j, T_a
(4)Check T_a-$T\leq \triangle T$
Compute
$SessK_{ab}' = f(h(ID_a), h(ID_b), M_j', T_a, T_b)$
(5)$E_{PKa}(h(ID_b)\oplus h(M_j'), M_j'\oplus h(M_j'), h(ID_b)\oplus T_b)$
(6)$D_{PKa}(h(ID_b)\oplus h(M_j'), M_j'\oplus h(M_j'), h(ID_b)\oplus T_b)$
if $M_j\oplus h(M_j)=M_j'\oplus h(M_j')$
Get $h(ID_b)$, $h(M_j')$, M_j', T_b
(7)Check T_b-$T\leq \triangle T$
Compute
$SessK_{ab} = f(h(ID_a), h(ID_b), M_j, T_a, T_b)$
(8)$E_{SessKab}$(Connection Request)
(9)$D_{SessKab}$(Connection Request)
(10)$E_{SessKab}'$ (Connection Reply)
(11)$D_{SessKab}'$ (Connection Reply)

Figure. 3. Authentication process.

V. Conclusion

This study proposes an improved authentication scheme based on previous complex computation processes; this scheme features enhanced privacy protection in OppNet environments. Results of the security analysis indicate that this scheme can stop tapping, forgery, and man-in-the-middle attacks and demonstrates superior security to other schemes. Regarding the functionality analysis, the proposed scheme exhibits comparatively fast and discrete protection to satisfy each of the aforementioned functions during message exchange processes between nodes. According to the performance analysis, more frequent message transmissions are required in the proposed scheme. However, the network environment of the proposed scheme is unsuitable for complex computations; therefore, increasing message transmission frequencies for reducing computational complexities is applicable for low-cost and energy-efficient devices

Acknowledgment

This research is supported in part by ROC MOST under contract number 101-2410-H-128-002, and Shih-Hsin University under contract numbers P10206 and P10307. The authors would like to thank their much help in this paper.

References

[1] B.Poonguzharselvi and V.Vetriselvi, “Data forwarding in Opportunistic Network Using mobile traces”, *International Conference on Information Technology Convergence and Services*, pp. 425–430, 2012.

[2] Dmytro Karamshuk, Chiara Boldrini, Marco Conti, and Andrea Passarella, “Human Mobility Models For Opportunistic Networks”, *IEEE Communications Magazine*, vol.49, issue 12, pp. 157-165, December, 2011.

[3] Er. Maggi Goyal and Er. Manoj Chaudhary，“Ensuring Privacy in opportunistic Network”, *Journal of Computer Engineering*, vol. 13, issue 2, pp. 74-82, 2013.

[4] Gianpiero Costantino, Fabio Martinelli, and Paolo Santi, “Privacy-Preserving Interest-Casting in Opportunistic Networks”, *IEEE Wireless Communications and Networking Conference: Mobile and Wireless Networks*, pp. 2829-2834, April , 2012.

[5] Iain Parris, Tristan Henderson, “Practical privacy-aware Opportunistic Networking”, *BCS Conference on Human-Computer Interaction*, vol. 25, pp. 553-557, 2011.

[6] Jian Ren, Yun Li, and Tongtong Li, “SPM: Source Privacy for Mobile Ad Hoc Networks”, *Journal on Wireless Communications and Networking*, doi: 10.1155/2010/534712, 2010.

[7] Luciana Pelusi, Andrea Passarella, and Marco Conti, “Opportunistic networking: data forwarding in disconnected mobile ad hoc networks“, *IEEE Communications Magazine*, vol. 44, no. 11, pp. 134-141, November 2006.

[8] Nicholas S. Samaras, Konstantinos Kokkinos, Costas Chaikalis, and Vasileios Vlachos, “On Intrusion Detection in Opportunistic Networks”, *anhellenic Conference on Informatics*, pp. 67-74, 2013.

[9] R. Di Pietro, S. Guarino, N.V. Verde, and J. Domingo-Ferrer, “Security in wireless ad-hoc networks – A survey”, *Computer Communications*, doi: 10.1016/j.comcom.2014.06.003, 2014.

[10] Wen-Chung Kuo, Hong-Ji Wei, and Jiin-Chiou Cheng, “An efficient and secure anonymous mobility network authentication scheme“, *Journal of Information Security and Applications*, vol. 19, issue 1, pp. 18-24, February, 2014.