ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

Efficient Hack ID Detection with Privacy Preserving Authentication in Wireless Mobile Networks

Neethu B [1], Nithin Joe [2]

P.G. Student, Department of Electronics and Communication Engineering, Nehru College of Engineering and Research Centre, Thrissur, Kerala, India[1]

Assistant Professor, Department of Electronics and Communication Engineering, Nehru College of Engineering and Research Centre, Thrissur, Kerala, India[2]

ABSTRACT: Roaming users travel across networks and hence user mobility is becoming an important network feature. The number of mobile services has a rapid increase and roaming service is a very important and convenient feature among them. The roaming service should be always secure because the users travelling across the network often want to hide the information like user id, location information etc. from other users and network. Any compromise in the privacy will result in attacker to reveal the user's identity and profile information, which can be exploited. Existing technologies focus on defending the leakage of information from attackers who can observe small traffic only. However, a strong adversary like a global eavesdropper can beat these existing methodologies. There are many protocols implemented for roaming services like two party, three party protocols etc. Some of these protocols take much computation time. The existing technology uses the Signcryption scheme, which has serious drawbacks. Signcryption minimizes the pseudo identities stored in the Subscriber Identity Module (SIM) and the authentication efficiency is also high when compared to the other protocols. However, there is a violation of identity in this protocol. That is, any user in a network can access the other network by accessing the id of users in that network. In this paper, we propose a new system for secure authentication using Receiver Signal Strength Indicator (RSSI). We propose a method to authenticate the users based on multiple parameters like transmission power, receiving power, energy level, position etc.

KEYWORDS: Roaming user privacy, Privacy preservation, Secure roaming services, RSSI technique.

I. INTRODUCTION

Recent years have witnessed a dramatic transformation in the mobile networks and industry. Mobile phone has become the dominant form of telecommunications. Mobile broadband has increased, smart phones and tablets are driving the trend to convergence. With the development of these services, mobile services have dramatically increased and provide more convenient life to its users. Among these services, roaming service is an important service. Roaming service helps the user to be associated with networks without any problem in accessing other services. The basic roaming service comprised of a home server (HS), a foreign server (FS) and a roaming user (RU). To make the roaming service secure, the home server should make sure the location privacy is assured for the roaming user. At the same time, the foreign server should be capable of authenticating the identity of real roaming user who requests for the service. The basic structure of a roaming service is as shown in the figure 1. The key security features of a roaming network are

1. Home Server and Foreign Server

There would be roaming agreement between Home Server (HS) and Foreign Server (FS) so only the registered users can access the data in the network. When a user wants to access the data in the network during roaming, the user needs

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

to register with the foreign server and authenticate. Security and privacy of user is very important, since there are chances the user characters like movement pattern, network usage habit may face privacy challenges.

2. Roaming Network Model

The roaming protocol consists of a Home Server (HS), Roaming User (RU), and a Foreign Server (FS) as shown in the figure. Each RU is registered with HS. Both HS and FS perform the private key generation. HS and FS create an agreement for roaming service and also create a roaming key. Each server and roaming user also has a unique signing key to use with the digital signature algorithm (ECDSA). All the servers will be synchronized at Greenwich Mean Time (GMT).

3. Anonymity and Signature Unforgeability

Authentication is required to ensure that roaming service is provided to only legitimate users. Hence roaming protocols provide a mutual authentication between the HS and FS. Signature algorithm used should be un forgeable by third parties and adversaries.

The roaming service should have a strong security protocol. Additionally, the security protocol of the roaming service should be proved in Canetti-Krawczyk model which is usually used to analyze key agreement between home server and the foreign server. Numerous protocols were proposed to preserve the privacy of roaming users in the recent years.

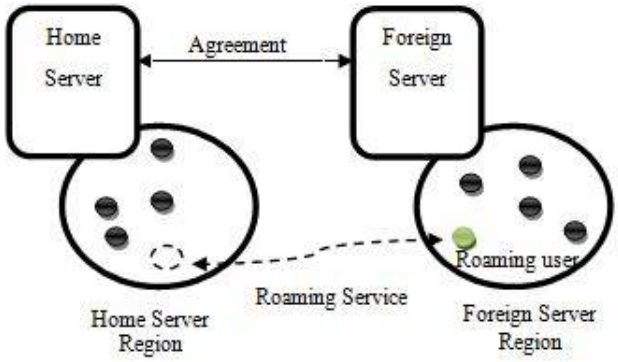

Fig. 1. Basic structure of a roaming network

II. LITERATURE SURVEY

G. Yang et al proposed the “universal authentication protocol for anonymous wireless communications” [2]. According to this work, there are two levels of user anonymity in a roaming service, weak user anonymity and strong user anonymity. In the weak user anonymity, the roaming user privacy is protected from the attacker/eavesdropper only. But in the strong user anonymity, the roaming user privacy is protected from eavesdropper as well as the foreign server. These two protocols have serious drawbacks. The first protocol does not provide strong user anonymity and the second protocol requires high computational cost. Additionally the second protocol does not support backward unlinkability. That is the information about a revoked user will not remain anonymous when the foreign server gets the roaming user’s revocation key.

To overcome these problems, D.He *et al* proposed a roaming protocol based on the group signature with backward unlinkability that results in high roaming authentication cost for the roaming user [3]. For backward unlinkability, it provides each user number of secret keys. The property of backward unlinkability becomes stronger as the number of secret keys increases. However, the revocation cost also increases with the number of users and secret keys. This time consuming operation at the server may be exploited by the attackers to perform a denial of service attack.

D. He *et al* also proposed a “secure and efficient handover authentication based on bilinear pairing functions” which is a pseudo identity based roaming protocol [4]. The protocol uses bilinear pairing operations to provide an efficient cryptographic system between foreign servers and roaming user. But his protocol does not have any

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

mechanisms to protect private key and the session key of roaming user from the eavesdropper. These keys can be computed from the messages that can be easily obtained by the eavesdropper.

According to G. Yang *et al* in "anonymous and authenticated key exchange for roaming networks", the type of protocol is not at all a problem [5]. In this work the authors put forward five properties that should be achieved for the strong user anonymity. The properties are (i) secure authentication which makes the user aware about the foreign server. (ii) Subscription validation which makes the foreign server assure about the roaming user. (iii) Key establishment where user and foreign server generate secret session keys. (iv) User anonymity in which the identity is known to the user and the home server only. (v) User untraceability in which only the roaming user and the home server knows the history of the user. This work also does a review of some of the related works [6, 7, 8] and finds they does not satisfy these properties. But unfortunately this protocol failed to be proven secure in CK model.

D. He *et al* proposed a lightweight roaming protocol in their work "Lightweight and provably secure user authentication with anonymity for the global mobility network" [9]. According to this, for roaming the user uses only a symmetric encryption algorithm and a hashing algorithm. It is an efficient protocol due to the use of lightweight algorithms. However, the protocol requires the participation of home server and it does not provide unlinkability. Another lightweight protocol was proposed in "a lightweight anonymous authentication scheme for VANET based on bilinear pairing" by H. Zhu *et al* [10]. Like the previous protocol, this protocol also depends on the home server which is a serious drawback.

Using the chameleon hash function, A. Shen *et al* proposed an efficient lightweight protocol in "a lightweight privacy preserving protocol using chameleon hashing for secure vehicular communications" [11]. In this protocol, a mobile node is authenticated by the foreign server by computing a chameleon hash function on the message sent by the node. These protocols have some security issues. Anyone can link the messages sent from the mobile node by using chameleon hash function since chameleon hash function on the messages are always identical.

The latest protocol was proposed by Hyo Jin Jo *et al* in their work "Efficient privacy-preserving authentication in wireless mobile networks" [12]. It is an efficient two party roaming protocol that guarantees effective anonymous authentication. This protocol uses a signcryption technique which is used for data encryption and creating digital signatures. Lower computational cost is a major advantage of using signcryption scheme. Use of signcryption scheme assures message confidentiality and signature unforgeability. Another advantage of this protocol is that it does not require home server support and the revocation process is real fast. Furthermore the protocol is secure in CK model. . One of the main advantage of this method is the use of pseudo ID's. Mainly these pseudo ID's provide anonymity ie, we can't trace the real identities by knowing the pseudo ID's. Usually it requires a large storage capacity of SIM card for storing the pseudo ID's but use of signcryption minimizes the number of pseudo ID's stored in the SIM. The architecture of this protocol is depicted in figure 2.

The signcryption based roaming protocol consists of two phases, First is an initial process phase and the next is an anonymous roaming system phase. Initial process phase composed of three steps (i) HS setup step, (ii) registration of RU step, (iii) roaming agreement step. In HS step, HS generates its own public parameters and secret values. In roaming agreement step each FS send their id to HS for computing a roaming key for all FS and the roaming key thus generated are transferred through a secure channel. Next in registration of RU step, the RU gets registered in the HS and will provide pseudo ID's and corresponding private keys. Anonymous roaming system phase composed of two steps, they are roaming protocol step and revocation step. In the roaming protocol step it satisfies all the requirements of roaming protocol such as authentication, unlinkability, anonymity, revocation etc. In the revocation step there comes two algorithms, update revocation list and revocation check.

Unfortunately, this protocol has some shortcomings like high communication, computational cost etc. There is also a violation of identity in this protocol. That is any user in the network can access the other network by accessing the user id in that network. This may lead the adversaries to impersonate as legitimate users by using their user id and perform Sybil attacks, man in the middle attack etc.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

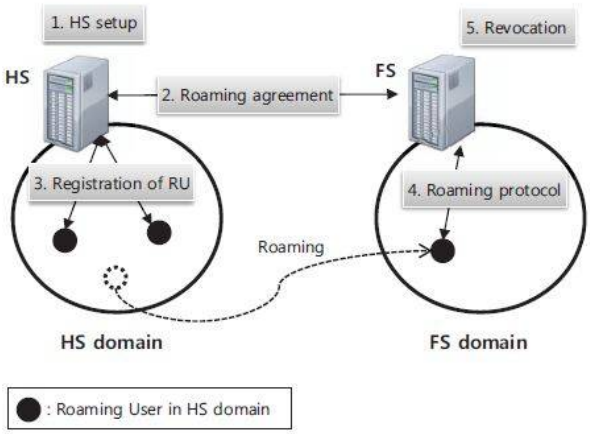

Fig. 2. Signcryption protocol overview

III. SYBIL ATTACK TO ROAMING NETWORKS

When a node illegitimately claims a different identity, or multiple identities, the network is said be under Sybil attack. The node may replicate in copies to confuse and collapse the network. There would be one to one mapping in a mobile network but Sybil attack violates this one to one mapping [13]. The node spoofing the identities of the nodes is called malicious node/Sybil attacker, and the nodes whose identities are spoofed are called Sybil nodes. The figure 3 shows a simple Sybil attack.

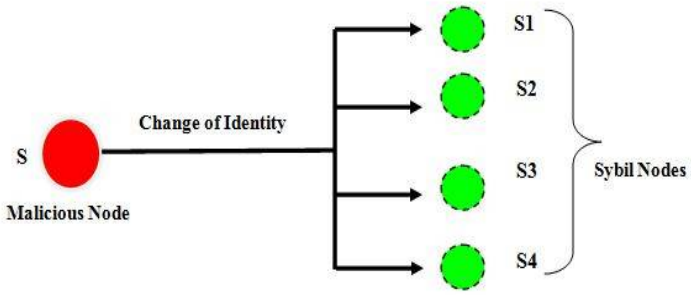

Fig. 3. Sybil attack with multiple identities

IV. PROPOSED SYSTEM

If any user from FS (Not a member of corresponding HS, Usually a hacker) takes any user's physical id (PID) and start communication, it is a violation of authentication and may cause serious troubles in the network. We propose a method to prevent such attacks in roaming networks.

According to our proposed system, the solution to this problem is during the registration phase, all the user properties get saved to HS. Each roaming user have its own properties like energy, power, position etc. these factors are hidden from other users. Authentication is based on properties also. A technique called RSSI (Receiver Signal Strength Indication) is used to compare the signal strength of the nodes. Figure 4 shows the block diagram of the proposed system.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

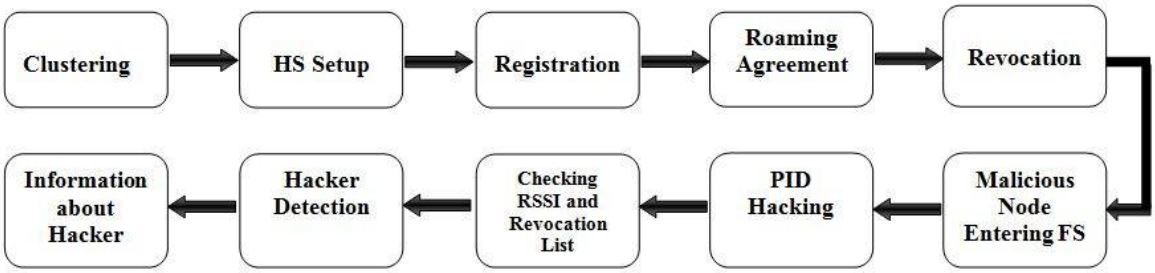

Fig. 4. Block diagram of proposed model

The steps involved in our model are as below:

- **Step 1 :** During registration step along with the physical ID, power, energy and position are also stored into the HS.
- **Step 2 :** On roaming, while sending the user details power, energy also gets transferred to the FS.
- **Step 3 :** Whenever a roaming user enter the FS it first check the revocation list and make confirm that the roaming user is get revoked.
- **Step 4 :** If any node hacks the PID and start communicating with the FS, then the FS calculates the signal strength, received power, energy and position.
- **Step 5 :** The obtained energy, power, position and signal strength are compared with the actual stored power and energy during registration phase.
- **Step 6 :** If there is any difference in the values then FS assumes it as a hacker.
- **Step 7 :** All nodes are informed about the hacker

V. SIMULATION RESULTS

The simulation of the system was performed in Network Simulator 2 (NS2). HS and FS were created with fixed number of nodes. The figure 5(a) shows the simulation of the registration phase. All the nodes are registered with the HS using the predefined user PID.

Once the registration phase is completed, one to one mapping of users is implemented. Each node starts sharing the details each other. The figure 5(b) shows the user information sharing.

In the third phase, user gets revoked from the HS and enters to the foreign network. Initially FS checks the revocation list and confirms the revocation. Revocation list is always updated by the HS whenever a user is revoked. If the node is malicious, then the FS do not provide access to the network. Revocation phase is shown in figure 5(c).

Suppose the malicious node hacks the PID of any other user and impersonates, then the FS checks the node power, energy, signal strength and position and compares with original node properties. If any variation is found, then it is assumed as an attacker.

Figure 5(d) shows the malicious client hacking the PID of a user and is being detected. Once the FS detects the malicious node, all other nodes are informed shown in figure 5(e). Once the malicious node is detected, it will be rejected from the corresponding network.

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

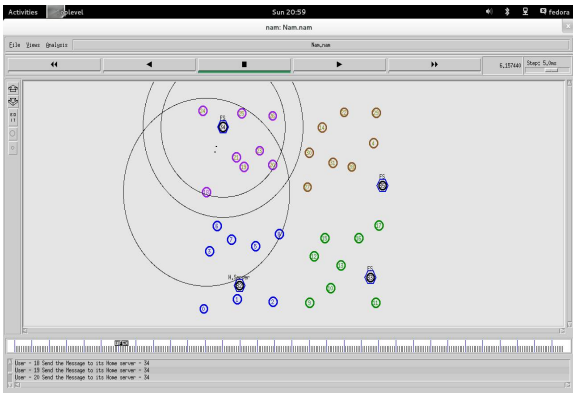

Fig. 5(a). Registration phase

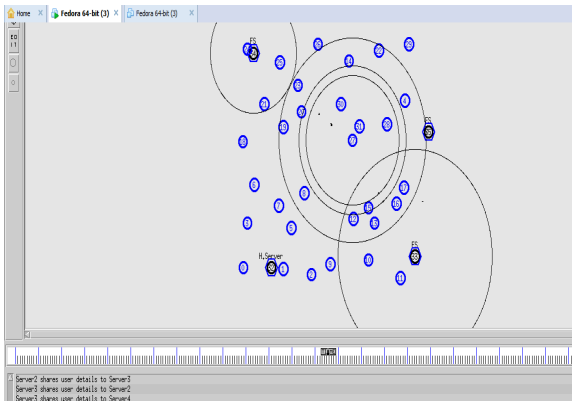

Fig. 5(b). User information sharing

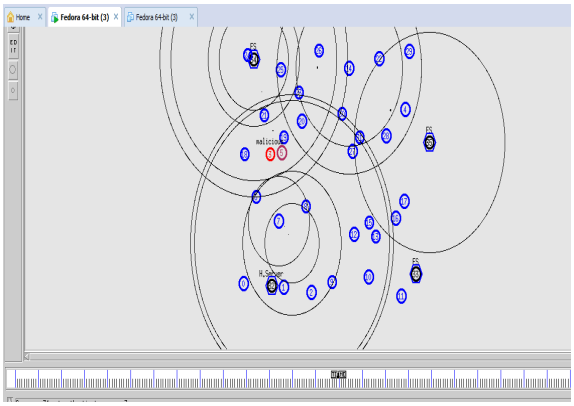

Fig. 5(c). Revocation of user

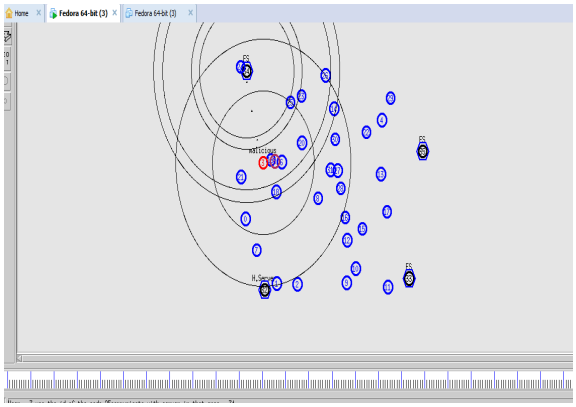

Fig. 5(d) PID hacking and detection

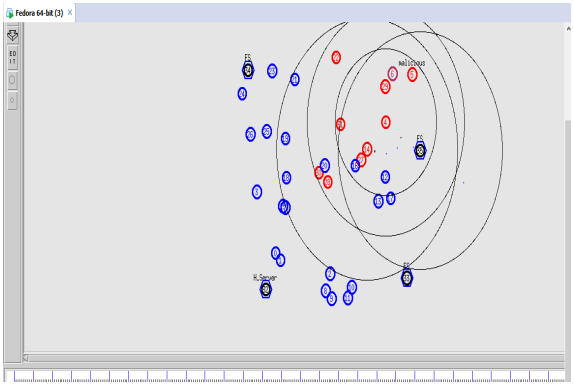

Fig. 5(e) FS alerts all other nodes about attack

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

VI. ANALYSIS

Based on the simulation results, different parameters of the system were analysed. Overhead, packet delivery ratio, throughput, and average energy consumption of the system were analysed.

1. Overhead

Overhead should be minimal for the better performance of the system. Our simulation results provided a very low overhead which shows the system is of high performance. The overhead graph is shown in figure 6 (a).

2. Packet Delivery Rate

Packet Delivery Rate is the ratio of number of delivered data packets to the destination. That is,

PDR=∑ no of packet received / ∑ no of packet sent

Greater the value of PDR means, better the performance of the system. Our simulation result gave high PDR result shown in figure 6(b).

3. Throughput

Throughput is the rate of successful message delivery over a communication channel. Our result shows high throughput. That is all messages reach at proper destination. Figure 6(c) shows the graph of throughput we got.

4. Average Energy Consumption

Average energy consumption is the ratio of total energy at time‘t’ to the total number of nodes active at time ‘t’. Here there is a gradual decrease in the average energy consumption as shown in the graph figure 6 (d) which proves our proposed system consume less energy and is of high efficiency.

5. Packet Drop

Packet drop occurs whenever the packet fails to reach destination. Drop reduces the throughput of the system. Our performance results show the system has very less packet drop. The figure 6(e) shows the graph of packet drop.

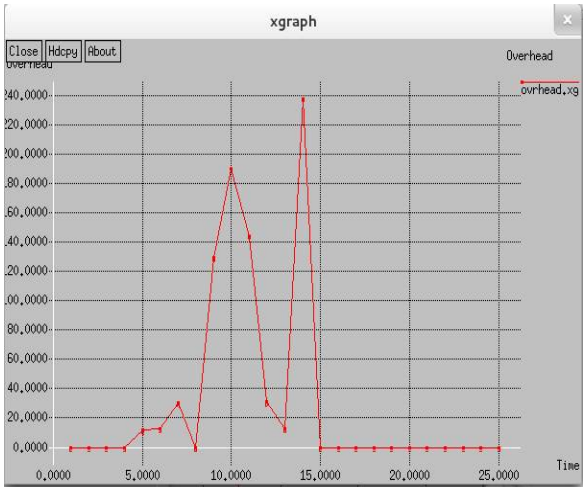

Fig. 6 (a) Overhead graph

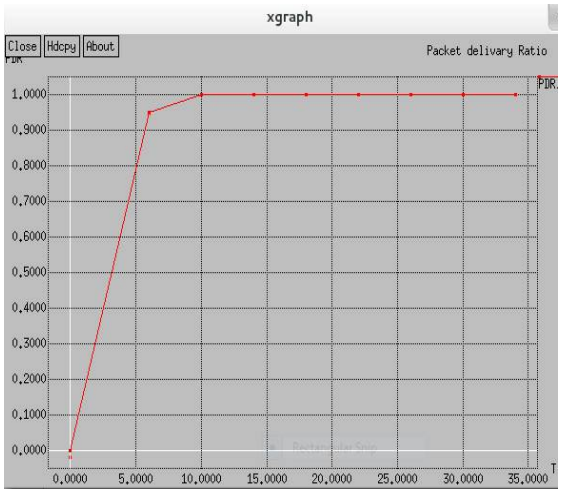

Fig. 6 (b) Packet Delivery Rate

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

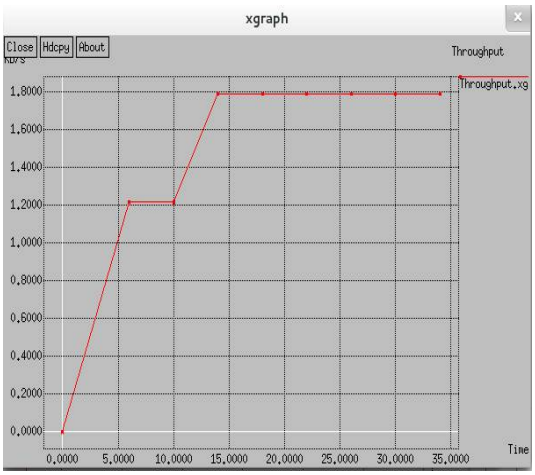

Fig. 6 (c). Throughput

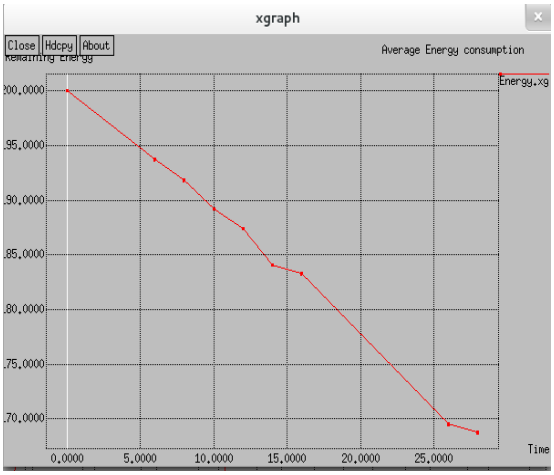

Fig. 6 (d). Average Energy Consumption

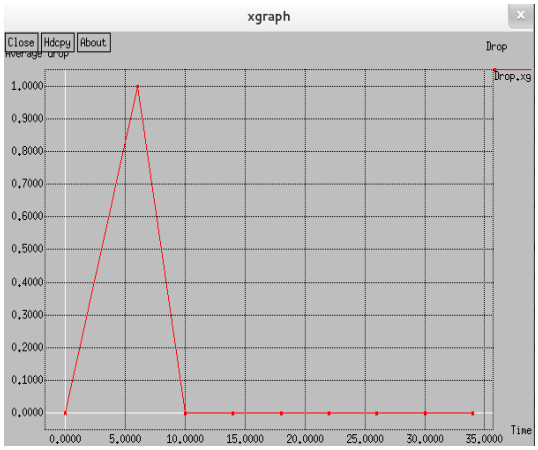

Fig. 6 (e) Packet drop

VII. CONCLUSION

We have designed a system which focuses on the security and privacy issues in wireless mobile networks. Sybil attacks and many other attacks like man in the middle attack, denial of service attack etc can be defended using our system. The proposed system will be effective against mobile number spoofing which is a serious threat to the network. This system can also be implemented on other mesh networks also. The simulation results of our system shows its best in performance and another advantage of the system is that this can be implemented on the existing system also.

REFERENCES

[1] Wikipedia, Wireless Networks, Available: https://en.wikipedia.org/wiki/Wireless_network
[2] G. Yang, Q. Huang, D. S. Wong, and X. Deng, "Universal authentication protocol for anonymous wireless communications," *IEEE Trans. Wireless Commun.*, vol. 9, no. 1, pp. 168–174, Jan. 2010.
[3] D. He, J. Bu, S. Chan, C. Chen, and M. Yin, "Privacy-preserving universal authentication protocol for wireless communications," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 431–436, Feb. 2011

ISSN(Online) : 2319-8753
ISSN (Print) : 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(An ISO 3297: 2007 Certified Organization)

Vol. 5, Issue 7, July 2016

[4] D. He, C. Chen, S. Chan, and J. Bu, "Secure and efficient handover authentication based on bilinear pairing functions," *IEEE Trans. Wireless Commun.*, vol. 11, no. 1, pp. 48–53, Jan. 2012
[5] G. Yang, D. S. Wong, and X. Deng, "Anonymous and authenticated key exchange for roaming networks," *IEEE Trans. Wireless Commun.*, vol. 6, no. 9, pp. 3461–3472, Sept. 2007
[6] D. Samfat, R. Molva, and N. Asokan, "Untraceability in mobile networks," in *Proc. MobiCom '95*, pp. 26–36
[7] J. Go and K. Kim, "Wireless authentication protocol preserving user anonymity," in *Proc. 2001 Symposium on Cryptography and Information Security (SCIS 2001)*, Jan. 2001, pp. 159–164
[8] K. F. Hwang and C. C. Chang, "A self-encryption mechanism for authentication of roaming and teleconference services," *IEEE Trans. Wireless Commun.*, vol. 2, no. 2, pp. 400–407, Mar. 2003
[9] C. Chen, D. He, S. Chan, J. Bu, Y. Gao, and R. Fan, "Lightweight and provably secure user authentication with anonymity for the global mobility network," *Int. J. Commun. Syst.*, vol. 24, no. 3, pp. 347–362, 2010
[10] H. Zhu, W. Pan, B. Liu, and H. Li, "A lightweight anonymous authentication scheme for VANET based on bilinear pairing," in *Proc. 4th Int. Conf. INCoS* Bucharest, Romania, 2012, pp. 222–228
[11] A. Shen, S. Guo, D. Zeng, and G. Mohsen, "A lightweight privacy preserving protocol using chameleon hashing for secure vehicular communications," in *Proc. IEEE WCNC*, Shanghai, China, 2012, pp. 2543–2548
[12] Hyo Jin Jo, Jung Ha Paik, and Dong Hoon Lee, "Efficient Privacy-Preserving Authentication in Wireless Mobile Networks," *IEEE Trans. Mobile Computing*, vol. 13, no. 7, pp. 1469–1481, Jul. 2014
[13] J.R. Douceur. The Sybil attack. In First International Workshop on Peer-to Peer Systems (IPTPS'02), Mar. 2002