RESEARCH ARTICLE OPEN ACCESS

REAL: A Reciprocal Protocol for Privacy in Wireless Communication Networks

Annapurna B P[1], Bhuvana N[2], Harshitha Rajendra[3], S Renukadevi[4]
UG Students [1], [2] & [3], Asst. Proff, [4]
Department Of Computer Science and Engineering
K S Institute of Technology
Bangalore - India

ABSTRACT

K-anonymity has been used to protect privacy in wireless communication networks, where intermediate nodes work together to report *k*-anonymized aggregate locations to a server. Each *k*-anonymized aggregate location is a cloaked area that contains at least *k* persons. In this paper, we propose a reciprocal protocol for privacy (REAL) in wireless communication networks. In REAL, nodes are required to autonomously organize themselves into a set of non-overlapping and highly accurate k-anonymized aggregate locations. The results show that REAL protects user information, provides more accurate query answers.

Keywords:- Reciprocity, information privacy, wireless communication networks, *k*-anonymity.

I. INTRODUCTION

In wireless communication network, user's information have privacy threats. If the attacker attacks the server as a result user's information is disclosed to the attacker. To tackle such privacy threats we are using k-anonymity to reciprocate the users details.

In this paper we propose a k-anonymity [1],[2],[3] to reciprocate the details. The objective is to generate reciprocated details of user in wireless communication networks.

To achieve security for user details we created a intermediate nodes between user and server. The k-anonymity is applied to user details at intermediate nodes to reciprocate. This reciprocated information is send to server. If attacker attacks the sever he gets reciprocated user information which is in server.

II. SYSTEM MODEL

The systemis divided into 4 different modules.

1. *User module:* Here user registers by filling the required details and user login to communicate. User sends query to intermediate node.
2. *Node module:* In this module the intermediate node is picked randomly after user login. Here k-anonymity to the users details is applied to reciprocate.
3. *Server module:* In this server receives the reciprocated user details from the intermediate node and also the query. It answers to the query.
4. *Attack module:* In this attacker attacks the server it gets reciprocated user details which is in server.

Here user registers into the network by filling the required details. After registration, user login to send a query. Once the user logs in single intermediate node is picked randomly among many intermediate nodes. Then k-anonymity is applied at the randomly selected intermediate node to generate reciprocated user details and that is send to the server. Then server answers the query and send it to intermediate node and this node send answer to the user *refer* Fig. 1.

If the attacker attacks server then the reciprocated user details in server is disclosed to the attacker. *Refer* Fig. 2.

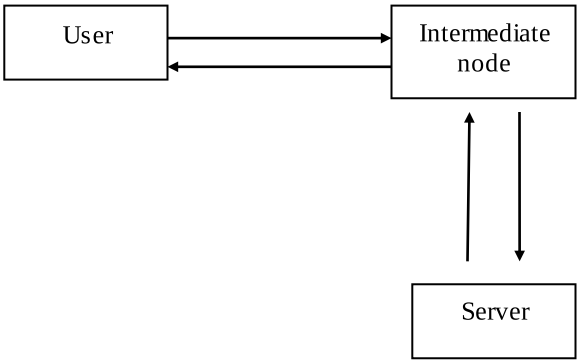


Fig. 1. Communication between user, intermediate node and server

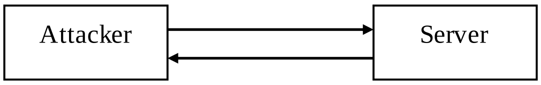


Fig. 2. Attacker attacks server and gets reciprocated user details

III. SYSTEM IMPLEMENTATION

In the proposed system, reciprocity protocol where the intermediate nodes execute reciprocity protocol for every reporting period to generate reciprocated user details by applying k-anonymity at intermediate node.

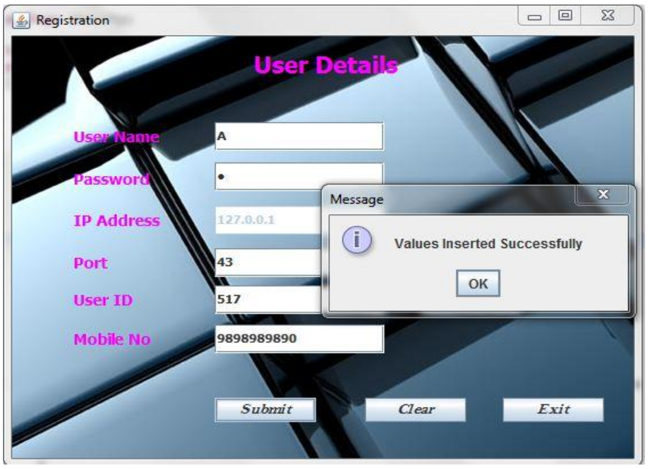
Initially the intermediate node is not created. Once the user login the intermediate node is generated. Among many nodes one node is picked randomly and it is used for communication between server and the user. The user communicates with server only through that randomly picked node.

In this, once the user communication ends or server is switched off the intermediate node which is picked randomly for that particular user is deleted automatically. In the database the intermediate node table is dropped automatically.

IV. RESULTS AND SNAPSHOTS

In the proposed system, the k-anonymity is applied to generate reciprocated user details. This has increased efficiency in terms of securing the user details from the attacker. Here if the server is attacked then the reciprocated details of user which is in server is received by the attacker. The users actual details is not disclosed to the attacker. This provides security to the user details. The answers obtained to the query are more accurate and delay time is less.

A. SNAPSHOTS


Registration

User Details

User Name: A

Password: •

IP Address: 127.0.0.1

Port: 43

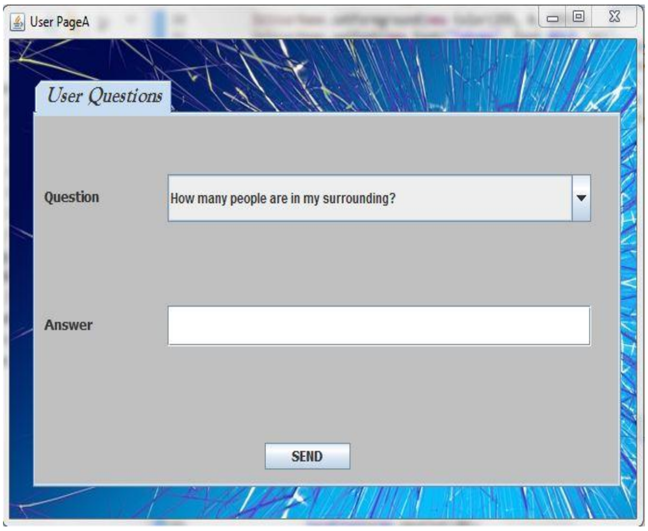
User ID: 517

Mobile No: 9898989890

Message

Values Inserted Successfully

Fig. 3: User Registration

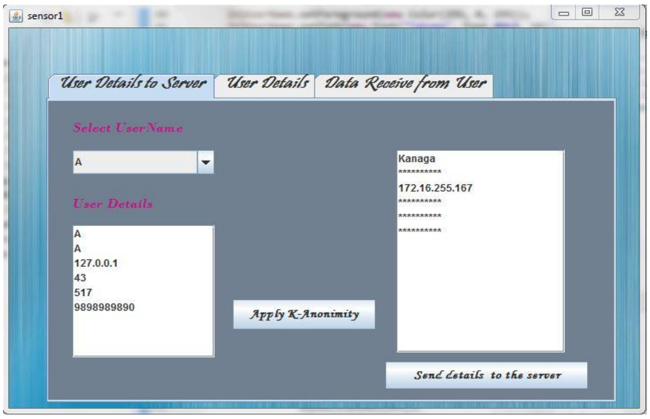

User PageA

User Questions

Question: How many people are in my surrounding?

Answer:

Fig. 4: User logged in and send query


sensor1

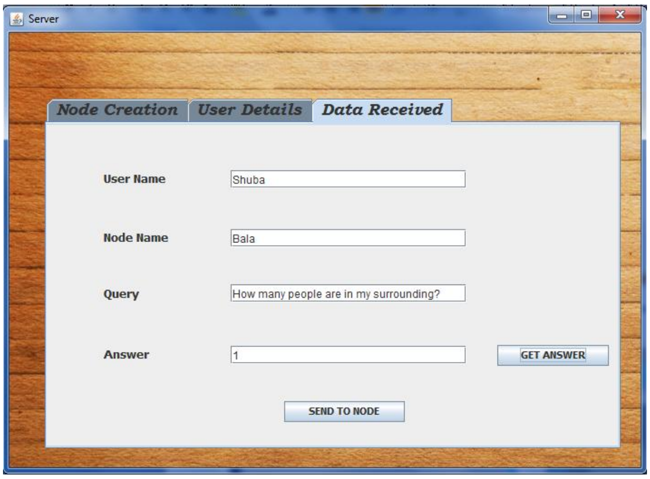
Select UserName: A

User Details

A
A
127.0.0.1
43
517
9898989890

Kanaga
****
172.16.255.167
****
****
****

Fig. 5: Applied k-anonymity at intermediate node



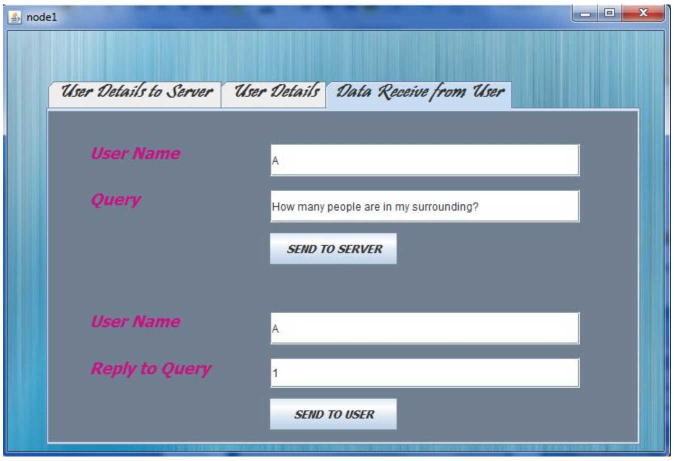
User Name Shuba

Node Name Bala

Query How many people are in my surrounding?

Answer 1

Fig. 6: Server received reciprocated user details and answers the query



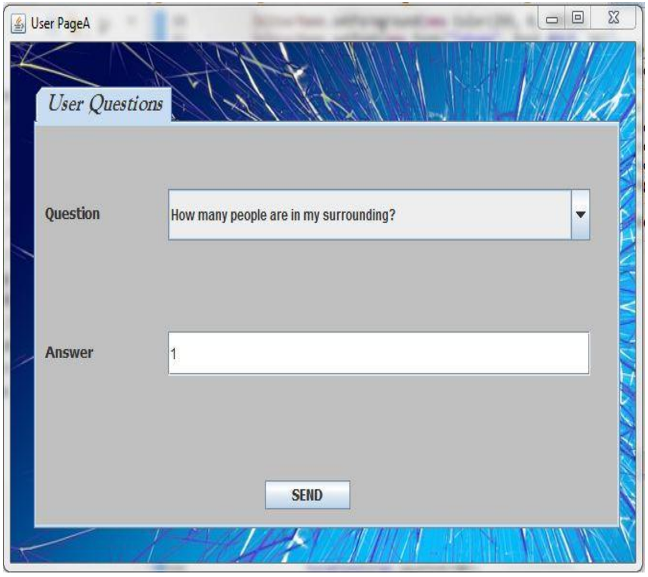
User Name A

Query How many people are in my surrounding?

User Name A

Reply to Query 1

Fig. 7: Answer to the query received by the intermediate node from server



Question How many people are in my surrounding?

Answer 1

Fig. 8: Answer to the query received by user from intermediate node

V. CONCLUSIONS

In this paper, we proposed that reciprocity property to secure users details in wireless communication networks. We defined an attack model that leads to a privacy breach in existing protocols because they generate overlapping. To avoid this privacy breach, REAL satisfies the reciprocity property by generating reciprocated users details by applying k-anonymity at intermediate node. We designed the process to accomplish self organisation of intermediate nodes to guarantee the reciprocity property and delay mechanism to improve the accuracy. By comparing with the state-of-the-art solutions, the results show that REAL protects users details and provides more accurate query answers and saves communication and computational costs.

ACKNOWLEDGMENT

Authors would like to thank K S Institute Of Technology for their support.

REFERENCES

[1] B. Bamba, L. Liu, P. Pesti, and T. Wang, “Supporting anonymous location queries in mobile environments with privacy grid,” in *Proc. 17th Int. Conf. World Wide Web*, 2008,pp.237-246.

[2] G. Ghinita, P. Kalnis, and S. Skiadopoulos, “PRIVE: Anonymous Location-based queries in distributed Mobile systems,” in *Proc. 16th Int. Conf. World Wide Web*, 2007, pp. 371-380.

[3] B. Hoh, T. Iwuchukwu, Q. Jacobson, D. Work, A. M. Bayen, R. Herring, J.-C. Herrera, M. Gruteser, M. Annavaram, and J. Ban, “Enhancing Privacy and accuracy in probe vehicle-based traffic monitoring via virtual trip lines,” *IEEE Trans. Mobile Comput.*, vol. 11, no. 5, pp. 849-864, May 2012.

[4] X. Pan, J. Xu, and X. Meng, “Protecting location privacy against location-dependent attacks in mobile services,” *IEEE Trans .Knowl. Data Eng.*, vol. 24, no. 8, pp. 1506-1519, Aug 2012.