IJRRECS/October 2013/Volume-1/Issue-6/ 1016-1019 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

DESIGN OF NETWORKS BASED ON THE URBAN VEHICLES AGAINST THE ATTACKS OF SYBIL ORIENTED FOOTPRINT

Ch.Santhosh laxmi[1], G.Balakrishna[2]

[1]M.Tech Student, Dept of CSE, Anurag Group of Institutions (formerly CVSR College of Engineering), Ghatkesar, R.R Dist, A.P, India

[2]Assistant Professor, Dept of CSE, Anurag Group of Institutions (formerly CVSR College of Engineering), Ghatkesar, R.R Dist, A.P, India

ABSTRACT:

Here the networks well oriented with respect to the urban vehicles plays a crucial role for the implementation of the system related to the aspects of the privacy is a major concern in the security based scenario of the vehicles oriented with respect to the anonymous phenomena of the privacy based location plays a crucial role in its representation is a major concern in the implementation of the system respectively. Where there is an indispensible vehicle anonymity takes place in the system beyond the verification of the users plays a crucial roe, respectively. Here the attacks are mainly used for the identification of the hostile multiple forging in addition with the scenario of the structured implementation of the analysis point of view in its relative strategy of the launch based attack of the Sybil plays a crucial role in its representation in a well oriented fashion respectively. Here in order to overcome the above problem a new technique is proposed based on the well oriented strategy of the implementation related to the efficient scenario of the effective structural oriented design of the unit base don the road side plays a crucial role in terms of the vehicles plays a crucial role for the attack based on the Sybil strategy respectively. Simulations have been conducted on the large number of the datasets in a different environments for the accurate analysis of the test bed based consideration plays a crucial role in its representation respectively. Here there is an accurate analysis of the implemented algorithm where there is an estimation of the performance followed by the outcome of the entire system in

a well stipulated fashion respectively.

Keywords: Attack of Sybil, Networks of the urbanized vehicles, Unit of the road side approach, Trajectory of the hidden location, Privacy of location and Signature of the ambiguous signer.

1. INTRODUCTION:

There is a lot of analysis takes place in the system in the research oriented scenario in a well stipulated fashion respectively [1][2]. Recently there is a huge research in the system takes place by the help of the analysis point of view related to the structural aspect of the network based on the vehicles plays a crucial role in its representation where there is a lot of advancement in the strategy of the cornerstone aspect of the system oriented with information technology is a major concern respectively [3][4]. There is a huge contribution regarding the analysis of the system in the unit of the road side strategy plays a crucial role for the anonymous tracking of the vehicles and its vehicular activities is a major concern in its related representation respectively [5][6]. Here the network well oriented with the vehicles plays a crucial role for the activities of the safety is a major concern apart from the implementation of the actions against the attacks in the road which is mainly on the driver seat as a major concentration respectively.

BLOCK DIAGRAM

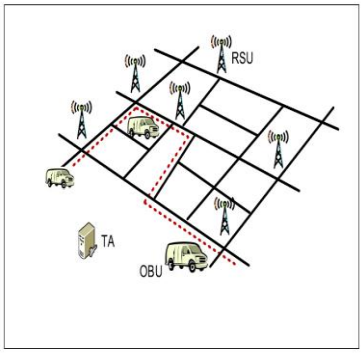

Fig1: shows the architecture of the present method respectively

2. METHODOLOGY:

Here the implementation of the present method is shown below in the block diagram based aspect and is explained in the brief elaborative fashion respectively [7][8]. Here the present method is implemented with a well efficient framework based

strategy in which there should be an improvement in the performance based strategy followed by the efficient outcome with a quite respective fashion [9][10]. There is a huge challenge for the present method in which it is supposed to accurately analyze the performance or the problem oriented strategy of the several previous methods and also the accurate outcome in a well respective fashion where there is a lot of the interest related to the theoretical based aspect respectively. Here the present method completely overcome the drawbacks of the several previous methods in a well efficient manner respectively. Here we finally conclude that the present method is effective and efficient in terms of the performance based strategy followed by the entire system based outcome in a well efficient manner respectively.

3. EXPECTED RESULTS:

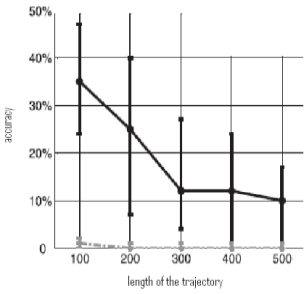

Fig2: shows the graphical representation of the present method respectively

A comparative analysis is made between the present method to that of the several previous methods in a well effective manner and is shown in the below figure in the form of the graphical representation and is explained in a brief elaborative fashion respectively. A lot of analysis is made on the present method and a huge number of the computations have been applied on the large number of the data sets in a well effective manner related to the different environmental aspect in a well efficient manner respectively. Here we finally conclude that the present method is effective and efficient n terms of the performance followed by the outcome in a well oriented fashion.

4. CONCLUSION:

In this paper a new technique is designed with a well efficient framework and by the help of the powerful strategy where there is an accurate implementation of the system in terms of the analysis followed by the outcome of the entire system in a stipulated fashion respectively. Here in the present strategy there is a lot of analysis takes place in the system by the effective implementation of the attack oriented to the respective Sybil plays a crucial role apart

from the development of the scheme related to the scenario of the network based on the urban vehicles plays a crucial role of the scheme oriented with the foot print plays a crucial role respectively. Here the messages based on the authorized consequences have been produced by the help of the vehicular based anonymity and the following unit of the RS plays a crucial role in its representation of the identification of the trajectory of the vehicle oriented correspondence plays a major role respectively. Vehicles related on the privacy of the location is completely oriented with the scheme of the hidden signature plays a crucial role of the local hidden strategy respectively. Here we finally conclude that the present method is effective and efficient in terms of the performance followed by the outcome of the entire system in a well oriented fashion respectively.

REFERENCES

[1] P. Maniatis, D.S.H. Rosenthal, M. Roussopoulos, M. Baker, T. Giuli, and Y. Muliadi, "Preserving Peer Replicas by Rate-Limited Sampled Voting," Proc. 19th ACM Symp. Operating Systems Principles (SOSP '03), pp. 44-59, Oct. 2003.

[2] H. Yu, M. Kaminsky, P.B. Gibbons, and A. Flaxman, "Sybilguard: Defending against Sybil Attacks via Social Networks," Proc. SIGCOMM, pp. 267-278, Sept. 2006.

[3] J.R. Douceur, "The Sybil Attack," Proc. First Int'l Workshop Peer-to- Peer Systems (IPTPS '02), pp. 251-260, Mar. 2002. CHANG ET AL.: FOOTPRINT: DETECTING SYBIL ATTACKS IN URBAN VEHICULAR NETWORKS 1113 Fig. 5. Trajectory length limit versus false positive error and false negative error. Fig. 6. RSU deployment versus false positive error and false negative error.

[4] J. Eriksson, H. Balakrishnan, and S. Madden, "Cabernet: Vehicular Content Delivery Using WiFi," Proc. MOBICOM '08, pp. 199-210, Sept. 2008.

[5] M. Castro, P. Druschel, A. Ganesh, A. Rowstron, and D.S. Wallach, "Secure Routing for Structured Peer-to-Peer Overlay Networks," Proc. Symp. Operating Systems Design and Implementation (OSDI '02), pp. 299-314, Dec. 2002.

[6] B. Dutertre, S. Cheung, and J. Levy, "Lightweight Key Management in Wireless Sensor Networks by Leveraging Initial Trust," Technical Report SRI-SDL-04-02, SRI Int'l, Apr. 2002.

[7] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," Proc. Int'l Symp. Information Processing in Sensor Networks (IPSN '04), pp. 259-268, Apr. 2004.

[8] S. Capkun, L. Buttyan, and J. Hubaux, "Self-Organized Public Key Management for Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 2, no. 1, pp. 52-64, Jan.-Mar. 2003.

[9] C. Piro, C. Shields, and B.N. Levine, "Detecting the Sybil Attack in Mobile Ad Hoc Networks," Proc. Securecomm and Workshop, pp. 1- 11, Aug. 2006.

[10] N. Borisov, "Computational Puzzles as Sybil Defenses," Proc. Sixth IEEE Int'l Conf. Peer-to-Peer Computing (P2P '06), pp. 171-176, Oct. 2006.