International Journal of Computing and Artificial Intelligence

E-ISSN: 2707-658X
P-ISSN: 2707-6571
IJCAI 2020; 1(2): 68-71
Received: 01-05-2020
Accepted: 05-06-2020

YL Prathapa Reddy
Head, Department of Computer Science, Sri Vijayadurga Degree College, Kurnool, Andhra Pradesh, India

Corresponding Author:
YL Prathapa Reddy
Head, Department of Computer Science, Sri Vijayadurga Degree College, Kurnool, Andhra Pradesh, India

Multimodal content protection information security situation awareness system based on PCCA

YL Prathapa Reddy

DOI: https://doi.org/10.33545/27076571.2020.v1.i2b.19

Abstract
Nowadays, many of these societies' data or texts (e.g., emails, messages posted in social media, healthcare outcomes, etc.) has become unstructured and semantic nature. This constitutes a challenge for automatic data protection methods. Hence, in this paper multimodal content protection information security situation awareness system based on PCCA is developed. In this position confidentiality conserving algorithm for content protection (PCCA) is used. The proposed algorithm applies computational intelligence for content protection by means of rule-based approach from computational intelligence and user's current position information. Hence, PCCA can efficiently conserve roaming user's position confidentiality while accomplishing better performance, guaranteed position confidentiality, and better quality of service.

Keywords: Position confidentiality, content protection, position confidentiality conserving algorithm (PCCA)

1. Introduction
Information technology has penetrated into all aspects of politics, economy, and culture of the whole society. The information revolution has changed the way of communication all over the world, promoted the giant development of human society, and also drawn unprecedented attention to network security issues. Studies, focusing on network security, have experienced four main stages: idealized design for ensuring security, auxiliary examination and passive defense, active analysis and strategy formulation, and overall perception and trend prediction [1]. Under the background of the new strategic command for the digital control that all countries are scrambled for, the discussion of network security situational awareness presents new characteristics both in the academic study and industrialization.

In this regard, a thorough investigation has been made in the present paper into the literature of network security situational awareness. Nowadays, Information and Communications Technology (ICT) have cemented the method for universal scale content sharing in e-Governance. Fundamentally, e-Governance or electronic governance is the application of ICT to the various procedures of Government functioning so as to achieve smart governance [2]. In general, e-Governance incorporates the use of ICTs by government organizations for:

a. Give-and-take of information with people, industries or several government sectors.
b. User confidentiality conserved, faster and effective provision of municipal facilities.
c. Refining the internal effectiveness and productivity.
d. Improving quality of services.

Government releases and transmits large volumes of electronic contents on day-to-day basis. But, these contents indicate private features of people (e.g., individuals inclinations, identities, ideas, current positions, etc.), hence triggering a severe content confidentiality risk. In order to avoid this risk, suitable content protection measures should be commenced by the authorities so as to accomplish with existing rules and regulations on content confidentiality.

Besides, user's position plays a vital role in a rapid growth of ICT applications causing the development of emerging e-Governance services and applications. With the fusion of position-based services and e-Governance; conserving user's position confidentiality is one of the most substantial objectives.

To achieve this objective, we offer a confidentiality conserving position-based query handling framework for content-protecting in e-Governance.

We identify several users of typical e-Governance services and applications which are Citizens, Enterprises, Businesses and Government. On the basis of users, e-Governances applications are categorized into four wide groups: Government to Citizens (G-C), Government to Enterprises (G-E), Government to Businesses (G-B) and Government to Government (G-G). It is important to use the aforementioned types of e-Governance services and applications through a secure mechanism. Hence, to achieve a user's position confidentiality in e-Governance; we propose a Position Confidentiality Conserving Algorithm (PCCA) in this paper. Data corruption instances specify that even the most prevailing service providers are not completely trustworthy [3-5]. This articulates content protection concerns of users.

2. Related work

In recent years, position-based services have been progressively incorporated into daily life and have subsequently conveyed people better convenience. To utilize position-based services, roaming users must send their service provider correct position information so as to accomplish the position-based query request. Generally, the position service provider's server is incredible, and the position information of the roaming user is susceptible to theft.

Subsequently stealing the position information of a roaming user, the intruder, by means of position tracking or links to supplementary public information for an instance geographical database may be able to authorize the roaming user's identity and achieve an improvement in extra confidential information. Several techniques have been introduced recently to guarantee the confidentiality protection of roaming users. These techniques can be divided into two groups: false position and spatial regions.

The model k-, earliest offered in the literature, denotes the anonymous position occurring when the position data of at least one other individual and the position information of k-1 cannot be distinguished. As a result, the individual's position to meet the position of k- turns out to be anonymous. The techniques discussed make use of a false position technique.

Our aim is to build a system archetype that satisfies the criteria of user's position confidentiality in the wireless search space area and allows users to query for e-Governance data on the basis of their current positions, while conserving their position confidentiality. In general, we want to support:

1. Point query to query for e-Governance data allied with a specific position.
2. Wireless search space area range query to query for e-Governance data allied with all positions in a specific range nearby the roaming user.
3. Adjacent neighbor query to query for e-Governance data allied with positions adjacent to a specified position. A. Computational Intelligence The conventional definition of the term computational intelligence (CI) does not exist even though it is used in different circumstances.

CI is defined as a discipline of artificial intelligence comprised of computer systems that makes use of numeric data, recognize patterns, display computational adaptability and fault tolerance, and commit errors at a rate approximating human performance. As per the directives from the IEEE Computational Intelligence Society, the conception of CI includes different topics of artificial intelligence covering the sub-areas of evolutionary multi-objective optimization, fuzzy inference systems, artificial neural networks and genetic algorithms.

The work can be explored with the concept of fuzzy logic for the user's uncertain behavior and position-based decision making. 1) Fuzzy Logic: The fuzzy set theory was presented by Zadeh in 1965 as an extension of multi-valued logic. It has been termed as a specific logic of fuzziness and approximate reasoning. The shape of the membership function defines the fuzzy set and is dependent on the purpose of set.

As far as the proposed work is concerned, we used fuzzy logic as a problem solving control system approach. Fuzzy logic offers a modest way of solving position-related queries containing ambiguous, vague, and imprecise input information. Furthermore, instead of applying a mathematical model to a particular system, fuzzy logic integrates a rule-based if A and B then C approach to solve position-based queries.

So, in the proposed framework, we integrate a rule-based approach to solve user's position-based queries in real time and to offer content protection in e-Governance. The position-based query forwarding and answering for content protection in e-Governance is implemented by means of the concept of a fuzzy inference system. We are using fuzzy logic as it is able to support real-time decisions about the context data of source nodes in wireless networks when such data has some degree of fuzziness and ambiguity. Consequently, conventional logic may lead to absolutely erroneous results owing to the ambiguity within context data. Fuzzy logic is a viable alternative to reasoning and making rational decisions with imprecision, uncertainty, incompleteness of information, conflicting information, partiality of truth and degrees of probability.

3. Proposed framework

The below figure (1) shows the proposed framework. The proposed framework is a four-stage technique for confidentiality conserving query handling.

Stage 1: Information forwarding
Stage 2: Position Confidentiality
Stage 3: Confidentiality conserving position monitoring framework
Stage 4: Quantum inspired hybrid intelligent position monitoring system in wireless networks
Stage 5: Search Space Based Multi Objective Optimization Evolutionary Algorithm
Stage 6: Least cloaked region scheming and authorization
Stage 7: PCCA

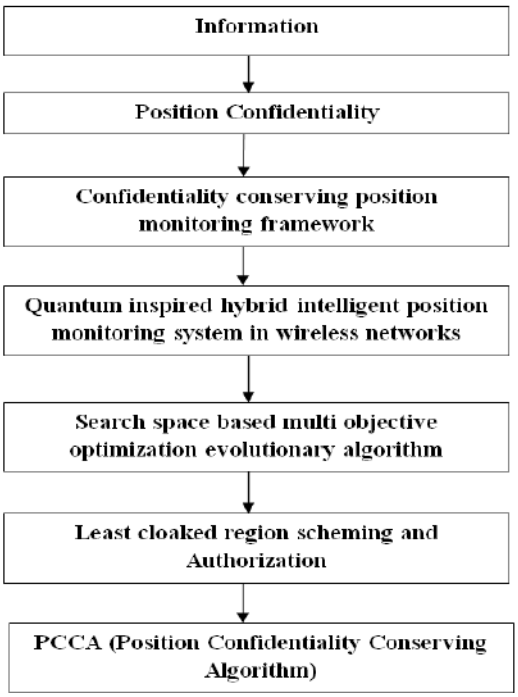

Fig 1: Proposed framework

Information forwarding is the initial stage where all spatially dispersed roaming users comprised in a specific wireless range area send a simple message to their respective neighboring users. As it is mentioned, the message contains the unique id of an individual roaming user for determination of an individual user uniquely, the wireless range area, and the total count of corresponding neighbor users involved in that particular wireless range area. It is compulsory for all roaming users to have their personal neighbor users list and to form a cluster of corresponding neighbor users.

The individual roaming user should conform their personal least cloaked region, which is basically the wireless range area that hides the confidentiality of the particular roaming user from illegal users (may be invaders). The position related information about a specific roaming user can be accessed by approved roaming users only which are contained within a particular least cloaked region. Therefore, it is crucial for all roaming users to arrange and conform their personal least cloaked region.

A cluster of authorized roaming users covered in the wireless search space area is treated as an input in this stage. This stage is meant for determination of the least cloaked region of a roaming user. It is important to check all the combinations and transformations of the roaming users in a wireless search space area. At least four roaming users should be grouped for the reason that a minimum of two roaming users is required to define the width of the least cloaked region and a minimum of two roaming users are required to define the height of the least cloaked region.

Least cloaked region scheming and authorization: Specific roaming user changes its wireless range area into a least cloaked region covering a minimum of k users for satisfying the prerequisite of k-anonymity confidentiality. Each roaming user arranges a search space area and determines a value for separate roaming user in its personal neighbor list. This value of roaming user is basically the ratio of the authorized neighbor user's count of a specific roaming user to the distance amongst roaming user and individual authorized neighbor user. In conclusion, roaming user formulates its least cloaked region, and this least cloaked.

The below figure (2) shows the quality of services and performance of proposed framework. By using proposed framework the both performance and services will be improved.

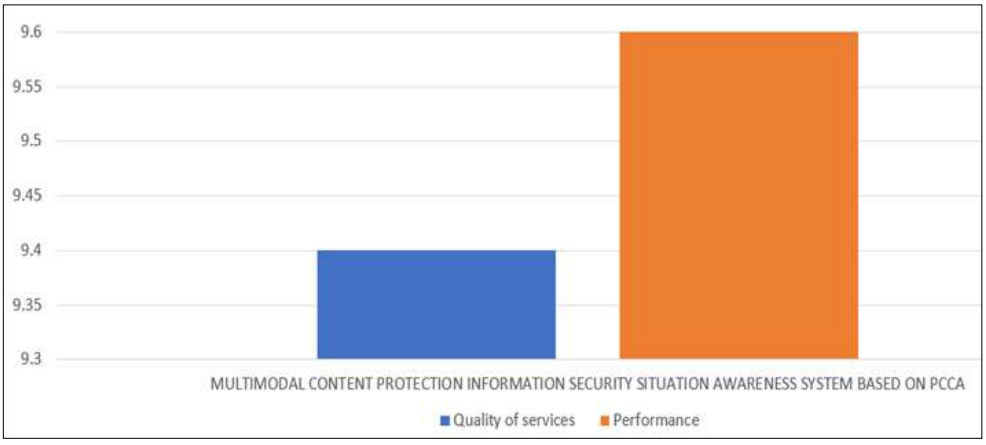

Fig 2: Quality of services and performance of proposed framework

4. Conclusion

Hence, in this paper multimodal content protection information security situation awareness system based on PCCA was developed. For content protection position confidentiality conserving algorithm (PCCA) is used. PCCA can organize roaming users into clusters with miscellaneous content interests, hence conserving their position confidentiality in e-Governance services and applications. The experimental results prove that PCCA achieves better performance, guarantees better position confidentiality and offers a quality of service more efficiently in comparison with the state-of-the-art confidentiality conserving position-based query handling algorithms while conserving roaming user's content confidentiality.

5. References

1. Medhane DV, Sangaiah AK. Source node position confidentiality aspects in wireless networks: An extended review. Int J High Perform Syst Archit 2016;6(2):61-81.
2. Medhane DV, Sangaiah AK. Source node position confidentiality (SNPC) conserving position monitoring system for wireless networks in Proc. Emerging ICT Bridging Future-Proc. 49th Annu Convention Comput Soc India CSI 2015;2:347-355.
3. Kamenyi DM, Wang Y, Zhang F, Memon I, Gustav YH. Authenticated privacy preserving for continuous query in location based services. J Comput Inf Syst 2013;9:24:9857-9864.
4. Gustav YH, Wang Y, Domenic MK, Zhang F, Memon I. Velocity similarity anonymization for continuous query location based services in Proc Int Conf Comput Problem-Solving 2013, P433-436.
5. Wang YLP, He Peng J, Zhang TT, Li HZ. Privacy preserving for continuous query in location based services in Proc IEEE 18th Int Conf Parallel Distrib Syst 2012, P213-220.
6. Yang K, Jia X. Data storage auditing service in cloud computing: Challenges, methods and opportunities. World Wide Web 2012;15(4)409-428.
7. Stenneth L, Phillip SY. Global privacy and transportation mode homogeneity anonymization in location based mobile systems with continuous queries, in Proc 6th Int Conf Collaborative Comput Netw Appl Worksharing 2010, P1–10.
8. Cellan-Jones R. The sidekick cloud disaster, BBC News 2009;1.
9. Miller R. Amazon addresses EC2 power outages. Data Center Knowledge 2010;1.
10. Pan X, Meng X, Xu J. Distortion-based anonymity for continuous queries in location-based mobile services, in Proc 17th ACM SIGSPATIAL Int Conf Adv Geographic Inf Syst 2009, 256-265.