स्थान आधारित सेवाओं (लोकेशन बेस्ड सर्विसेज) में 'क-गोपनीयता' के माध्यम से उपयोगकर्ताओं की गोपनीयता का संरक्षण

Privacy Protection in Location Based Services using K-Anonymity

रुबीना शाहीन जुबैरी[1], दिनेश चंद्र[2]
Rubina Shahin Zuberi, Dinesh Chandra
आई टी एस, इंजीनियरिंग कॉलेज, गौतम बुद्ध नगर, ग्रेटर नॉएडा, उत्तर प्रदेश
rshahinz@gmail.com; dinesshc@gmail.com

सारांश

बेतार संचार प्रणालियों में स्थान आधारित सेवाओं के आगमन से गोपनीयता को मिलने वाली चुनौतियों के बारे में उपयोगकर्ता के लिए एक बढ़ती हुई चिंताओं का विषय उठाया गया है। उपयोगकर्ता अपने स्थान समन्वय ग्लोबल पोजिशनिंग सिस्टम (जी. पी. एस.) के माध्यम से स्थान आधारित प्रश्न के रूप में जो जानकारी देता है, यह जानकारी अगर किसी को पता चल सकती है तो उस से गोपनीयता भंग हो जाती है। इन मुद्दों पर कई तकनीकें आई हैं जिनमें क - गोपनीयता (K-ANONYMITY) को अध्ययन करने के विभिन्न रूपों और विभिन्न संदर्भों में सबसे व्यापक रूप में इस्तेमाल किया गया है। इस लेख में हम एल.बी.एस. (लोकेशन बेस्ड सर्विसेज) और हाल ही में एल.बी.एस. की प्रगति के लिए क - गोपनीयता (K-ANONYMITY) की समीक्षा को प्रस्तुत कर रहे हैं। एलबीएस में क - गोपनीयता (K-ANONYMITY) की उपयोगिता के लिए तीन दृष्टिकोणों को मान्यता दी गई है, वे हैं - संचार प्रणाली की वास्तुकला के आधार पर, सॉफ्टवेयर के एल्गोरिदम पर आधारित और क - गोपनीयता (K-ANONYMITY) यानि सही नाम न छापने के प्रकार के आधार पर (विभिन्न क्वेरी के अनुसार प्रोसेसिंग तकनीक)। यह समीक्षा इन दृष्टिकोणों की रूपरेखा के भीतर की गई है। यह समीक्षा अपने वर्तमान इस्तेमाल की तकनीक में नवीनतम तकनीकों और संभव संशोधनों के साथ गोपनीयता प्रदाताओं की मदद कर सकती है।

ABSTRACT

The advent of location based services in wireless communication systems has raised a growing concern for the user about privacy. The queries of a user in Location Based Services (LBS) may reveal its position to the server. This server stores Global Positioning Systems (GPS) query information which becomes a privacy breach. As there are different servers pertaining to different services, it becomes hard to enable privacy measures in all of them. There are several techniques emerging on privacy protection in LBS. K-Anonymity is widely popular amongst them. Here we are summarizing most of the k-anonymity techniques available and their emerging trends. Here we have also tried to compare the present and popular k-anonymity techniques on the basis of its applicability for privacy protection in LBS systems. The three perspectives – architecture, algorithm and the ways

of cloaking have been elaborated. This has been done to analyze and protect the user's privacy at all the possible levels of the LBS systems. This protects the user robustly as hardware as well as software enhancements may provide unprecedented protection to the LBS users and will certainly improve its utility.

मुख्य शब्द: स्थान आधारित सेवा या एल.बी.एस. (लोकेशन बेस्ड सर्विसेज), ग्लोबल पोजिशनिंग सिस्टम (जी. पी. एस.), क-गोपनीयता।

Key words : Location Based Services (LBS), Global Positioning Systems (GPS), K-Anonymity.

परिचय

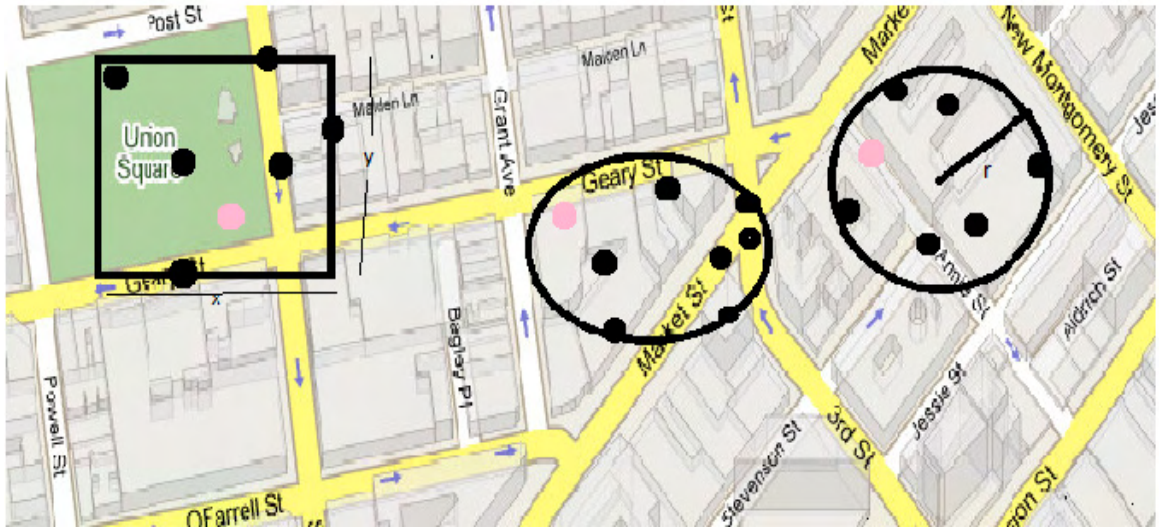
आजकल प्रत्येक स्मार्टफोन पर जीपीएस आधारित लोकेशन बेस्ड सर्विस मिल जाती है। स्मार्टफोन पर आपकी लोकेशन, उसका रिकॉर्ड और फिर किसी ऐप तक वो जानकारी पहुंचना कोई नई बात नहीं है। कभी-कभी हमें पता होता है कि क्या जानकारी हमारे स्मार्टफोन से ली जा रही है, लेकिन कई बार आपको पता भी नहीं चलता और स्मार्टफोन से जानकारी चली जाती है।

आप कैमरे से जो भी तस्वीर लेंगे, कैमरा मेटा डेटा में तस्वीर के बारे में जानकारी रहती है, फोटो की लोकेशन, दिन-तारीख़ और समय ये डेटा दिखाई नहीं देगा लेकिन फेसबुक जैसे ऐप पर जैसे ही इसे शेयर करेंगे, ये जानकारी उस तस्वीर से ली जा सकती है। अगर आपने ऐसी कोई तस्वीर ऑनलाइन पोस्ट कर दी, तो उसके बारे में पता करना बहुत मुश्किल नहीं है। फेसबुक पर एक फीचर है 'नियर बाई फ्रेंड्स', जो आपको और आपके दोस्तों की लोकेशन एक दूसरे को बताता है। आप यहां पर अपने लोकेशन को एक या दो घंटे के लिए शेयर करने की इजाजत दे सकते हैं।

इतने समय में अगर कोई दोस्त उस जगह मिल गया, तो वो आपको ढूंढ सकता है। लेकिन अगर ये जानकारी सार्वजानिक हो गई तो चोर उचक्के उसका फायदा उठा सकते हैं। ट्विटर पर अपने अकाउंट की सेटिंग करते समय अगर आप थोड़ी सावधानी से लॉग इन नहीं कर रहे हैं, तो आपके हर पोस्ट के साथ लोकेशन भी आ जाती है। कई मेसेजिंग ऐपों पर जब भी आप अपना मैसेज भेजते हैं, तो आपके लोकेशन से जुड़ी जानकारी उसमें शामिल होती है। इसको चेक करने के लिए आप 'सेटिंग' में जाइये, उसके बाद 'प्राइवेसी' चुनना होगा और फिर 'लोकेशन सर्विसेज'। उसके बाद आपको 'शेयर माई लोकेशन' दिखाई देगा, जहां पर आप इसे ऑन या ऑफ कर सकते हैं। कई डेटिंग सर्विस ऐप पर आपके लोकेशन की जानकारी भी ली जाती है। ऐसे ऐप का कहना है कि वो चाहते हैं कि आपके पसंद का कोई पार्टनर आपके इलाक़े में ही मिल जाए। इसलिए लोकेशन की जानकारी लेना जरूरी है। कभी-कभी तो ये आपसे रियल टाइम लोकेशन अपडेट भी लेने की कोशिश करते हैं। ऐसी जानकारी देना ख़तरनाक हो सकता है और ऐसे ऐप के लिए लोकेशन को ऑफ कर के रखना ही सुरक्षा के हित में होगा।

लोकेशन बेस्ड सर्विसेज में लागू होने वाली क-गोपनीयता

क-गोपनीयता (K-ANONYMITY) की उत्पत्ति डेटाबेस एनालिसिस [40] में हुई है, यह उपयोगकर्ता को क-1 एवं अन्य उपयोगकर्ताओं के



चित्र 1: डेटा दूरी निर्भर क्लोकिंग का उदाहरण (गुलाबी बिंदु उपयोगकर्ता विचाराधीन और काले डॉट्स अन्य उपयोगकर्ता इंगित करते हैं) [43]

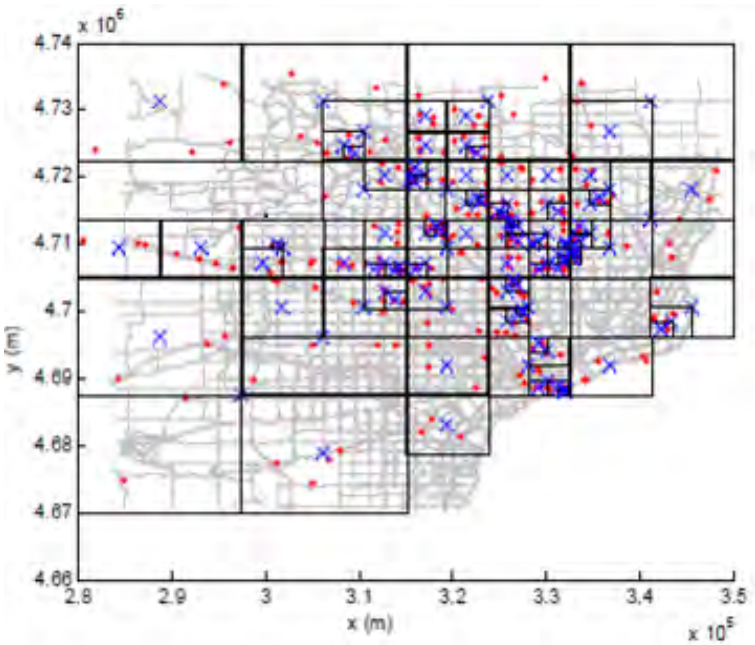
साथ गुमनामित करता है। गोपनीयता सुनिश्चित करने के लिए क-गोपनीयता (K-ANONYMITY) लागू करने के लिए तीन दृष्टिकोणों पर विचार किया जाना चाहिए: (i) एलबीएस आर्किटेक्चर जिसमें क-अनामता/गोपनीयता का इस्तेमाल किया जाएगा (ii) गोपनीयता के प्रकार या आवेदन के प्रकार तथा (iii) एल्गोरिदम, क्वेरी प्रसंस्करण तकनीकों के आधार पर।

तीन दृष्टान्त

पहला परिप्रेक्ष्य: आर्किटेक्चर

संचार प्रणाली के आर्किटेक्चर में दो मुख्य संभावनाएं हैं जो एलबीएस को क-गोपनीयता (K-ANONYMITY) प्रदान कर सकती हैं: अनाम नामांकन के लिए एकल भरोसेमंद सर्वर [4], [6], [7], [8], [9], [10], [11], [12] और वितरण के लिए पीयर (जहां उपयोगकर्ता को विश्वासयोग्य दल माना जाता है और वे निनामी-गुमनामी करते हैं [15], [17], [18], [19], [20] । हालांकि इन बुनियादी आर्किटेक्चर के कुछ नुकसानों को दूर करने के लिए मिश्रित आर्किटेक्चर का भी उपयोग किया जाता है, जैसे: विश्वसनीय सर्वर विफलता का एक बिंदु है और पीयर के सभी उपयोगकर्ताओं पर अँधा विश्वास है।

क्लस्टर भरोसेमंद अनामकरता (सीटीए), दोनों ही क्लाइंट और सर्वर का नाम निवारण करने के लिए इस्तेमाल किये गए। ओथमान एवं अन्य [14] द्वारा सीटीए प्रस्तावित किया गया था। दोनों क्लाइंट और सर्वर पर दो मॉडयूल लागू किए गए थे, एक सर्वर प्लेट पर विश्वसनीय प्लेटफॉर्म मॉडयूल (टीपीएम) है और दूसरा विश्वसनीय मोबाइल मॉडयूल है क्लाइंट पर (एमटीएम) टकाबी आदि [1] ने एक वितरित आर्किटेक्चर का प्रस्ताव किया जो एक मुख्य सर्वर और कई उप-सर्वर (एलबीएस प्रदाता) का उपयोग करता है। मुख्य सर्वर में कुल क्षेत्र की पूरी जानकारी होती है जिसमें एलबीएस प्रदान किया जाता है, जबकि उप-सर्वर अपने कक्षों में उपयोगकर्ताओं को अनमोल कर देते हैं। झोंग एवं अन्य [5] ने एक अन्य क-गोपनीयता (K-ANONYMITY) प्रस्ताव पेश



चित्र 2: स्थानिक क्लोकिंग का स्नैपशॉट जीपीएस ट्रेल्स पर लागू होता है [39]

किया है जो यह मानता है कि कई सर्वर हैं, प्रत्येक एक अलग संगठन द्वारा तैनात किया गया है ताकि वे अपना स्थान साझा कर सकें और एक केन्द्रक की गणना कर सकें, जो वे अपने नकली स्थान के रूप में उपयोग करते हैं। एस जेन्सेन एवं अन्य [16] किसी भी विश्वसनीय तृतीय पक्ष सर्वर का उपयोग किए बिना, पारंपरिक क्लाइंट-सर्वर आर्किटेक्चर में काम करते हैं। लेखक ने गैर-केंद्रीकृत संचार [20] को समर्थन देने के लिए प्रवर्तित की भी विधि है वे एक मॉडयूलर दृष्टिकोण का प्रस्ताव करते हैं, जो उत्तरदायी रूप से उपयोगकर्ताओं द्वारा हासिल की जाने वाली गोपनीयता को बढ़ाता है। बुनियादी मॉडयूल फेरर [18] द्वारा प्रस्तावित विधि के बराबर है, जहां उपयोगकर्ता प्रत्येक तीसरे मॉडयूल पर भरोसा करते हैं, जो उपयोगकर्ताओं की गारंटी के लिए गोपनीयता समरूपता का उपयोग करता है। ऐसा देखा गया है कि दो मूल आर्किटेक्चरों की प्रयोज्यता मिश्रित आर्किटेक्चर से कम है। दरअसल, मूल आर्किटेक्चर के इस संकरण (Hybridization) को उपयोगकर्ताओं और मौजूदा संचार प्रणाली के साथ एलबीएस आर्किटेक्चर की संगतता बढ़ाने के लिए चित्र में लाया गया है। सामान्य रूप से इन आर्किटेक्चरों की तुलना संभव नहीं है, जबकि किसी विशेष संचार परिदृश्य के अनुरूप उन्हें संशोधित किया जा सकता है।

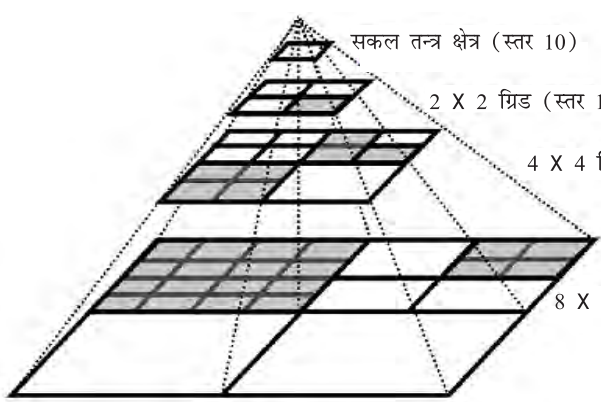
दूसरा परिप्रेक्ष्य: एल्गोरिदम

क-गोपनीयता (K-ANONYMITY) एल्गोरिदम डेटाबेस से अपनी उत्पत्ति तथा तकनीक का विश्लेषण करती है। एलबीएस में आवेदन करने के लिए उन्हें संशोधित किया जाता है और कई नामों के लिए एल्गोरिदम भी तैयार हो गए हैं। इन एल्गोरिदमों को 'क्लोकिंग रणनीतियों' के रूप में भी जाना जाता है। इन्हें दो श्रेणियों में वर्गीकृत किया जा सकता है: (i) डेटा निर्भर क्लोकिंग, (ii) क्षेत्र निर्भर क्लोकिंग। डेटा निर्भर क्लोकिंग प्रणाली में प्रत्येक उपयोगकर्ता के वास्तविक स्थान और अनुरोध के स्थान से उसकी दूरी के आधार पर अज्ञातता के क्षेत्र तैयार किये जाते हैं। विशेष रूप से, दूरी आधारित क्लोकिंग एल्गोरिदम [13, 25, 27] अनुरोधकर्ता के क-1 निकटतम पड़ोसियों को पुन: प्राप्त करते हैं और एक ऐसा क्षेत्र उत्पन्न करते हैं जिसमें सभी क-उपयोगकर्ता शामिल होते हैं। इस सीमा क्षेत्र का आकार पूर्वनिर्धारित नहीं है, लेकिन अब तक अधिकांश आयताकार और अंडाकारों का इस्तेमाल है [23] (चित्र 1)। क्षेत्र पर निर्भर क्लोकिंग गुमनामी के क्षेत्रों को तैयार करने के लिए निनामी (nonymizer)

द्वारा कवर किए गए कुल क्षेत्र को ध्यान में रखते हैं (चित्र 2)। विशेष रूप से, ग्रिड आधारित क्लोकिंग [8, 11, 28] ग्रिड फैशन में क्षेत्र का विभाजन करती है और ग्रिड के प्रत्येक कक्ष में उपयोगकर्ताओं को पुनः प्राप्त करते हुए (अनुरोधकर्ता के सेल से शुरू करती है और पड़ोसी कोशिकाओं में जाती है) कम से कम अज्ञातता का क्षेत्र उत्पन्न करती है (चित्र 1)। गादिक और लियू [7] भरोसेमंद सर्वर क्लीक् क्लोक नामक एक क-गोपनीयता (K-ANONYMITY) एल्गोरिदम का उपयोग करते हैं, जो एक अप्रतिबंधित ग्राफ के आधार पर अनुरोध के एक सेट के लिए एक विस्तारित क्षेत्र खोजता है- इस आलेख में नोड्स को अप्रसारित अनुरोधों के सेट द्वारा दर्शाया जाता है। यदि अनुरोध अलग-अलग उपयोगकर्ताओं के हैं और अनुरोध के स्थान डेटा दूसरे की सहिष्णुता बाधाओं के भीतर हैं तो दो नोड्स (अनुरोध) जुड़े हुए हैं । जब कोई अनुरोध प्राप्त होता है, तो उसे ग्राफ में जोड़ा जाता है और एल्गोरिदम क (अनुरोध में निर्दिष्ट) का पता लगाने की कोशिश करता है जिसमें 'बेस' अनुरोध शामिल होता है। लेकिन, क्लिक क्लोक सेवा की गुणवत्ता को प्रभावित कर सकता है, क्योंकि, अनुरोध के कुल प्रसंस्करण में पर्याप्त देरी हो जाती है। जिसके कारण कुछ अनुरोधों में काफी देरी हो सकती है, जबकि अन्य प्रश्नों को बेकार मान के छोड़ दिया जा सकता है। कलनीस एवं अन्य [6] का एल्गोरिदम केंद्र क्लोक एक दूरी आधारित दृष्टिकोण है। सेंटर क्लोक का एक संस्करण है निकटतम क्लोक (एनएन-क्लोक) [7] जो उत्पन्न स्थान के बारे में अनिश्चितता प्रदान करता है।

कैस्पर और इसका संशोधित न्यू कैस्पर [11] स्थान के लिए लोकप्रिय ग्रिड-आधारित तकनीकों में से हैं।

अंतराल क्लोक [8] कैस्पर के समान है क्योंकि यह एक क्वाड-ट्री में डेटा का आयोजन भी करता है। हालांकि, अंतराल क्लोक एक ही स्तर पर पड़ोसी कोशिकाओं पर विचार नहीं करता है। इसके बजाय यह सीधे पिरामिड में पिछले स्तर तक जाता है। दोनों अंतराल क्लोक और कैस्पर को समान डेटा वितरण के लिए ही लागू किया जा सकता है। स्टार क्लिक [34] में नोड विकसित की गयी है जो x होस्ट, और y हमलावरों की संख्या होगी। बेन एवं अन्य [41] ने क्लोकिंग का एक अलग तरीका इस्तेमाल किया है। उन्होंने एंट्रोपी मेट्रिक के आधार पर इन डमी स्थानों को चुना है। उन्होंने यह सब सुनिश्चित करने के लिए एक उन्नत डीएलएस एल्गोरिदम का प्रस्ताव किया है जो चयनित डमी स्थानों को यथासंभव फैलाते हैं। नटेसन और लियू [42] ने उपयोगकर्ताओं की गोपनीयता सेटिंग्स के प्रबंधन के लिए एक नया दृष्टिकोण लिया। उन्होंने एक रूपरेखा विकसित की है जो प्रयोक्ताओं को अपनी गोपनीयता प्राथमिकताओं को प्रभावी ढंग



चित्र 3 : द न्यू कैस्पर द्वारा क्वाड-ट्री पार्टीशनिंग द्वारा बनाई गई अपूर्ण पिरामिड छायांकित क्षेत्र उपयोगकर्ता की उपस्थिति दिखाता है। [43]

से चुनने और प्रबंधित करने में मदद करेगा और गुमनामियों से संदर्भ-आधारित गोपनीयता प्राप्त करने में मदद करेगा। आमतौर पर गोपनीयता प्रोफाइल के चुनाव को प्रभावित करने वाले कारकों के एक समूह के विश्लेषण के आधार पर, उपयोगकर्ताओं को अपने स्थान-आधारित गोपनीयता की सुरक्षा के लिए सही निर्णय लेने में सहायता करने के लिए एक सीखने का मॉडल बनाया गया है।

अब तक परिकलित एल्गोरिदम एक विश्वसनीय सर्वर के लिए डिजाइन किए गए हैं कुछ संशोधनों के साथ ये एल्गोरिदम कुछ अन्य आर्किटेक्चर के अनुरूप हो सकते हैं। उनकी वास्तविक गुणवत्ता मानदंड गोपनीयता के खिलाफ उनकी मजबूती हैं। इसलिए हाल ही में प्रस्तुत अधिकांश एल्गोरिदम कुछ या अन्य एलबीएस परिदृश्य में उनकी प्रयोज्यता प्राप्त करते हैं।

तीसरा परिप्रेक्ष्य : क-गोपनीयता (K-ANONYMITY) के प्रकार

प्रश्न प्रसंस्करण तकनीकों के आधार पर प्रश्नों की मात्रा और उनकी प्रतिक्रिया अलग-अलग होती है इसलिए एल्गोरिदम को तदनुसार संशोधित करने की आवश्यकता होती है। जब उपयोगकर्ता स्थानांतरित और स्थान आधारित क्वेरी का अनुरोध करता है तो क्वेरी के उत्तर देने में लिया गया समय उपयोगकर्ता के लिए उपयोगी होने के लिए पर्याप्त होना चाहिए। एक स्थान से अनुरोध 'स्थान' क-गोपनीयता (K-ANONYMITY) तकनीक, निरंतर क्वेरी या स्थान अंक के सेट से संबंधित अनुरोध (जहां उपयोगकर्ता को चलाना माना जाता है) को पथ क-गोपनीयता (K-ANONYMITY) कहा जाता है, और जब उपयोगकर्ता के पिछले स्थानों को अनमनीकरण (Disentanglement) की प्रक्रिया के लिए भी माना जाता है तब 'ऐतिहासिक' क-गोपनीयता (K-ANONYMITY) तस्वीर में आती है। अनुरोधकर्ता के एकल स्थान को लेने वाली प्रणाली में क-गोपनीयता (K-ANONYMITY) का परिचय केवल 'स्थान' आधारित कहा जा सकता है। एलबीएस में गोपनीयता संरक्षण पर अनुसंधान की शुरुआत में केवल स्थान क-गोपनीयता (K-ANONYMITY) को लगभग सभी रिपोर्ट [4, 5, 6, 7] में माना गया था। स्थान क-गोपनीयता (K-ANONYMITY) एल्गोरिदम कुछ संशोधनों के साथ ऐतिहासिक तथा पथ क-गोपनीयता (K-ANONYMITY) तकनीकों में इस्तेमाल किये जा सकते हैं।

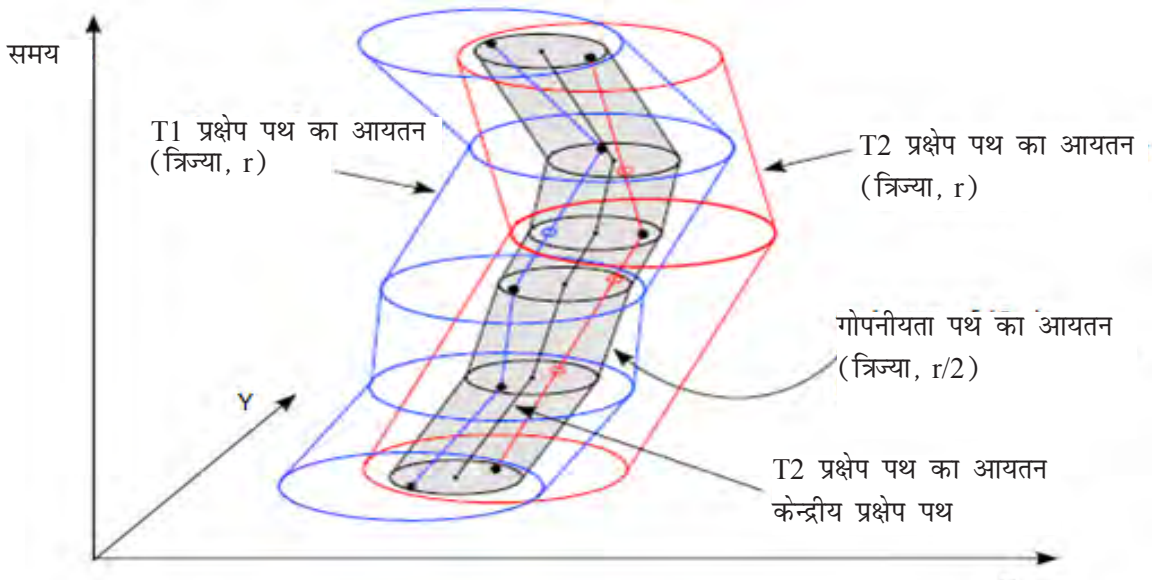
'पथ' क-गोपनीयता (K-ANONYMITY) पहले चो और मोकबेल [24] द्वारा प्रस्तावित की गयी थी जिन्होंने स्नैपशॉट (एकल स्थान) की अवधारण ा को लगातार पूछताछ के लिए बढ़ाया और ट्रैजेक्टरी (पथ) के इस नए डोमेन का नाम-बोधन किया। तालिका 1 रोगियों का ट्रैजेक्टरी डेटा प्रदर्शित करती है। इन आंकड़ों से, प्रतिद्वंद्वी के विषय में का पता चलता है कि वह (1, 5) का दौरा समय 2 पर और

RID	Trajectory	Disease	...
1	$(1,5,2) \rightarrow (6,7,4) \rightarrow (8,10,5) \rightarrow (11,8,8)$	HIV	...
2	$(5,6,1) \rightarrow (3,7,2) \rightarrow (1,5,6) \rightarrow (7,8,7) \rightarrow (1,11,8) \rightarrow (6,5,10)$	Flu	...
3	$(4,7,2) \rightarrow (4,6,3) \rightarrow (5,1,6) \rightarrow (11,8,8) \rightarrow (5,8,9)$	Flu	...
4	$(10,3,5) \rightarrow (7,3,7) \rightarrow (4,6,10)$	HIV	...
5	$(7,6,3) \rightarrow (6,7,4) \rightarrow (6,10,6) \rightarrow (4,6,9)$	Fever	...

तालिका 1: रोगियों का ट्रैजेक्टरी डेटा

(8,10) का दौरा समय 5 पर समझ रहा है। इस से यह फैसला किया जा सकता है कि इस रोगी को एचआईवी है।

निरंतर एलबीएस अनुरोधों को संसाधित करने के लिए, दो मुख्य दृष्टिकोण हैं:- (i) एक एलबीएस अनुरोध प्रत्येक समय आवृत्ति के लिए बार-बार प्रस्तुत किया जाता है जब तक कि यह समाप्त नहीं हो जाता है, इस प्रकार लगातार परिणामों के मूल्यांकन की आवश्यकता होती है, और (ii) अगर भविष्य के बारे में जानकारी प्रदान की गई है तो क्वेरी परिणाम की केवल गणना की जाती है । पहला दृष्टिकोण नमूनाकरण (यदि नमूना दर बहुत कम है तो परिणाम गलत होगा) की कमी से ग्रस्त है [26] । इसलिए क्वेरी परिणामों के बारे में कोई गारंटी नहीं है। चो और मोकबेल [24] ने निरंतर प्रश्नों के लिए एल्गोरिदम बनाया जो इन लक्ष्यों को प्राप्त कर सकते हैं : (i) स्थान गोपनीयता और क्वेरी गोपनीयता (ii) अलग-अलग क साझा क्षेत्र और याद रखने का गुण (iii) निरंतर स्थान-आधारित प्रश्नों का समर्थन करना। ताउ एवं अन्य [32] निरंतर प्रश्नों की संभावना के बारे में सोचने वाले पहले अन्वेषक थे। शिन एवं अन्य [35] ने दिखाया कि विरोधी अब उपयोगकर्ता के प्रक्षेप वक्र को ट्रैक कर सकता है, इससे संभावना हुई कि उपयोगकर्ता की संवेदनशील जानकारी प्रकट हो सकती है। सॉंग एवं अन्य [34] उन उपयोगकर्ताओं को स्थानांतरित करने के लिए निकटतम पड़ोसी (एनएन) खोज एल्गोरिदम प्रदान करता है जो आर-ट्री (R-tree) का उपयोग करते हैं जैसे कि ऐतिहासिक जानकारी [36] भंडारित संरचनाएं। जीकोलालस एवं अन्य [28] एक दृष्टिकोण प्रस्तावित करता है जो उपयोगकर्ता के अक्सर उपयोग किए जाने वाले मार्गों को पहचानता है और संग्रहीत करता है। अबुल एवं अन्य [31] के काम में उपयोगकर्ता गतिशीलता को एक पथ नहीं माना गया था, लेकिन एक बेलनाकार राशि थी जो



चित्र 4 : (2, r) नाम न छापने वाले दो सह-स्थानीय कृत प्रक्षेपिकों द्वारा गठितय त्रिज्या और के साथ उनकी अनिश्चितता की मात्रा और केंद्रीय अनिश्चितता खंड जिसमें त्रिज्या r/2 के साथ दोनों प्रक्षेप पथ trajectories शामिल हैं [43]

उपयोगकर्ता के सटीक पथ की अनिश्चितता का पता लगाता है और एक समान बेलनाकार पथ (चित्र-4) में एक उपयोगकर्ता से अधिक होने पर गुमनामी मानी जाती है। निस्संदेह स्थान अज्ञातता मूल क-गोपनीयता (K-ANONYMITY) तकनीक है और यह सभी उपलब्ध एलबीएस आर्किटेक्चर और एल्गोरिदमों के साथ सबसे अधिक अनुकूल है। लेकिन मोबाइल संचार प्रणालियों के प्रक्षेपण के साथ-अज्ञातता (कुछ स्थितियों में ऐतिहासिक के साथ) एक बेहतर व्यवहार्य निनामी समाधान प्रस्तुत करती है।

क-गोपनीयता (K-ANONYMITY) के माध्यम से गोपनीयता में संभव भावी रुझान

अब तक जो काम किया गया है, वह क-गोपनीयता (K-ANONYMITY) के सभी तीन दृष्टिकोणों अर्थात इस का आर्किटेक्चर, उसके एल्गोरिदम और इसके प्रकार में व्यापक गुंजाइश रखता है। धारणाएं जैसे कि उपयोगकर्ता द्वारा भावी पथ के प्रावधान या उपयोगकर्ता द्वारा हर क्वेरी से पहले क्वेरी के कुछ मापदंडों को स्थापित करने से अधिक दिशा निर्देशों से अधिक सैद्धांतिक दृष्टिकोणों के लिए व्यावहारिक दिशा निर्देश प्राप्त होते हैं। इन बुनियादी समस्याओं के समाधान को और अधिक व्यावहारिक रूप से प्राप्त करने की दिशा में काम करने से एलबीएस प्रणाली की दृढ़ता में सफलता प्राप्त हो सकती है जो निश्चित रूप से उनकी लोकप्रियता को प्रोत्साहित करेगी।

सन्दर्भ (References)

[1] H. Takabi, J.B.D. Joshi and H.A. Karimi, "A collaborative *k*-anonymity approach for location privacy in location based services" in 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing, 2009, pp. 1 – 9.

[2] M. Duckham and L. Kulit, "A formal model of obfuscation and negotiation for location privacy", in Proceedings of International Conference of Pervasive Computing (LNCS), Munich, pp. 152-170, 2005.

[3] C. A. Ardagna, M. Cremonini, E. Damiani, S. D. C. Vimercati, P. Samarati, "Location privacy protection through obfuscation-based techniques", in S. Baker, G.Ahn, eds.: Data and Applications Security, pp. 47-60, 2007.

[4] B. Gedik, L. Liu, "Protecting location privacy with personalized *k*-anonymity: Architecture and algorithms", IEEE Transactions on Mobile Computing, vol. 7, pp. 1-18, 2008.

[5] G. Zhong and U. Hengartner, "Toward a Distributed *k*-Anonymity Protocol for Location Privacy", in Proc. of the Workshop on Privacy in the Electronic Society, USA, 2008, pp. 33-37.

[6] P. Kalnis, G. Ghinita, K. Mouratidis, and D. Papadias, "Preserving Anonymity in Location Based Services", Technical Report TRB6/06, School of Computing, The National University of Singapore, 2006.

[7] B. Gedik and L. Liu, "Location Privacy in Mobile Systems: A Personalized Anonymization Model", in Proceedings of 25th International Conference on Distributed Computing Systems, 2005, pp.620–629.

[8] M. Gruteser and D. Grunwald, "Anonymous Usage of Location-Based Services Through Spatial and Temporal Cloaking", in Proceedings of 1st International Conference on Mobile Systems, Applicationsand Services,2003, pp.31–42.

[9] A.Kapadia,N.Triandopoulos,C.Cornelius, D. Peebles, and D. Kotz, "AnonySense: Opportunistic and Privacy-Preserving Context Collection",in Proceedings of 6th International Conference on Pervasive Computing, 2008, pp.280–297.

[10] S. Mascetti and C. Bettini, "A Comparison of Spatial Generalization Algorithms for LBS Privacy Preservation", in Proceedings of International Workshop on Privacy-Aware Location-based Mobile Services, 2007.

[11] M. F. Mokbel, C.Y. Chow, and W. G. Aref, "The New Casper: Query Processing for Location Services without Compromising Privacy", in Proceedings of 32nd International Conference on Very Large Data Bases, 2006, pp. 763–774.

[12] P. Paillier, "Public-Key Cryptosystems Based on Composite Degree Residuosity Classes", in Proceedings of EUROCRYPT '99, 1999,pp.223–238.

[13] C. Bettini, S. Mascetti, X. S. Wang, and S. Jajodia, "Anonymity in Location-based Services: Towards a General Framework", in Proceedings of 8th International Conference on Mobile Data Management, 2007, pp. 67–79.

[14] H.Othman , H. Hashim , J. A. Manan, "Privacy Preservation in Location-Based Services (LBS) Through Trusted Computing Technology", in Proceedings of the 2009 IEEE 9th Malaysia International Conference on Communications, 2009, Kuala Lumpur, Malaysia.

[15] P. K.G. Ghinita, S. Skiadopoulos, "Prive: anonymous location based queries in distributed mobile systems", in Proceedings of 16th International World Wide Web Conference,2007,pp. 371-380.

[16] H. L. a. M. L. Y. C. S. Jensen, "Location Privacy Techniques in Client-Server Architectures", Lecture Notes in Computer Science, vol. 5599, pp. 31-58, 2009.

[17] C. Chow, M. F. Mokbel, X. Liu, "A peer-to-peer spatial cloaking algorithm for anonymous location-based services", in Proc. of the 14th annual ACM international symposium on Advances in geographic information systems, Virginia, USA, 2006, pp. 171-178.

[18] J. Domingo-Ferrer, "Microaggregation for database and location privacy", in O. Etzion, T. Kuflik, A. Motro, eds.: Next Generation Information Technologies and Systems, pp. 106-116, 2006.

[19] A. Solanas, A. Martinez-Balleste, "Privacy protection in location-based services through a public-key privacy homomorphism", in Proc. of the 4th European PKI Workshop: theory and practice, 2007, pp.362-368.

[20] A. Solanas, A. Martinez-Balleste, "Location privacy in location-based services: Beyond TTP-based Schemes", in Proc. of the 1st International Workshop on Privacy in Location-Based Applications, Spain, 2008.

[21] T. Okamoto, S. Uchiyama, "A new public-key cryptosystem as secure as factoring", in Proc. of the Advances in Cryptology EUROCRYPT'98, 1998.

[22] M. Duckham, L. Kulit, Location Privacy and Location-Aware Computing, in Dynamic and Mobile GIS: Investigating Changes in Space and Time, CRC Press, pp. 35-52, 2007.

[23] A. Gkoulalas-Divanis, P. Kalnis, V.S.Verykios, "Providing *k*-anonymity in

Location based services", ACM SIGKKD Explorations Newsletter, vol.12,2010.

[24] C. Y. Chow and M. F. Mokbel, "Enabling private continuous queries for revealed user locations", in Proceedings of the 10th International Symposium on Advances in Spatial and Temporal Databases ,2007, pp.258-275.

[25] A. Gkoulalas-Divanis, V. S. Verykios, and M. F. Mokbel, "Identifying unsafe routes for network based trajectory privacy", in Proceedings of the SIAM InternationalConference on Data Mining (SDM), SIGKDD, 2009.

[26] Y. Tao, D.Papadias and J.Sun, "The TPR*-tree: an optimized spatio-temporal access method for predictive queries", in Proceedings of the 29th international conference on Very Large Data Bases, vol. 29,2003, pp.790–801.

[27] P. Zacharouli, A. Gkoulalas-Divanis and V. S.Verykios, "A *K*-anonymity model for spatiotemporal Data", in Proceedings of the IEEE Workshop on Spatio- Temporal Data Mining (STDM), SIGKDD, 2007, pp. 555-564.

[28] A. Gkoulalas-Divanis and V. S. Verykios,"A free terrain model for trajectory *K*-anonymity" , in Proceedings of the 19th International Conference on Database and Expert Systems Applications 2008, pp. 49-56.

[29] C. Bettini, X. S. Wang, and S. Jajodia, "Protecting Privacy Against Location-Based Personal Identification", in Proc. of the 2nd VLDB Workshop on Secure Data Management, Springer-Verlag, 2005, pp. 185-199.

[30] H. Samet,The Design and Analysis of Spatial Data Structures, Addison-Wesley Longman Publishing Co.,Inc., 1990.

[31] O.Abul, F.Bonchi and M. Nanni, "Never Walk Alone: Uncertainty for Anonymity in Moving Objects Databases", International Conference on Data Engineering - ICDE, 2008, pp. 376-385.

[32] Y. Tao, D. Papadias, and Q. Shen, "Continuous nearest neighbor search," in proceedings of Very Large Data Bases, 2002, Hong Kong, pp. 287–298.

[33] K. P. N. Puttaswamy, A. Sala and B. Y. Zhao, "Star Clique: Guaranteeing User Privacy in Social Networks Against Intersection Attacks", in proceedings of ACM Against Intersection Attacks", in proceedings of ACM CoNEXT, 2009, Rome, ITALY.

[34] Z. Song and N. Roussopoulos , "*K*-Nearest Neighbor Search for Moving Query Point", in Proceedings of Symposium on Advances in Spatial and Temporal Databases, 2001.

[35] H. Shin, J. Vaidya, V. Atluri and S. Choi, "Ensuring Privacy and Security for LBS through Trajectory Partitioning", in Eleventh International Conference on Mobile Data Management, IEEE Computer Society, 2010.

[36] Y. Manolopoulos, A. Nanopoulos, A. N. Papadopoulos and Y. Theodoridis, R-trees: Theory and Applications, Springer-Verlag, 2005.

[37] C. Bettini, X.S. Wang, S. Jajodia, "Protecting privacy against location-based personal identification", in Proceedings of the 2nd VLDB Workshop on Secure Data Management, 2005, pp. 185–199.

[38] A. Gkoulalas-Divanis, V. S. Verykios and P. Bozanis, "A network aware privacy model for online requests in trajectory data", Data & Knowledge Engineering, pp. 431-452, 2009.

[39] B.Hoh, Achieving guaranteed anonymity in time series location data, PhD Thesis, University of New Jersey, pp.46.

[40] G.Aggarwal, T. F`eder, K. Kenthapadi, R. Motwani, R. Panigrahy, D. Thomas and A. Zhu, "Approximation algorithms for *k*-anonymity", in Proceedings of the 10th International Conference on Database Theory, 2005.

[41] Niu, Ben, Qinghua Li, Xiaoyan Zhu, Guohong Cao, and Hui Li. "Achieving k-anonymity in privacy-aware location-based services." In *INFOCOM, 2014 Proceedings IEEE*, pp. 754-762. IEEE, 2014.

[42] Natesan, Gayathri, and Jigang Liu. "An adaptive learning model for k-anonymity location privacy protection." In *Computer Software and Applications Conference (COMPSAC), 2015 IEEE 39th Annual*, vol. 3, pp. 10-16. IEEE, 2015.

[43] Zuberi, Rubina Shahin, Brejesh Lall, and Syed Naseem Ahmad. "Privacy protection through k. anonymity in location. based services." *IETE Technical Review* 29, no. 3 (2012): 196-201.

* * *

वर्ष 2017 के विज्ञान संबंधी नोबेल पुरस्कार

प्रत्येक वर्ष की तरह ही वर्ष 2017 के भी नोबेल पुरस्कारों की घोषणा कर दी गई है। विज्ञान विषयक पुरस्कार विजेताओं और उनके योगदान संबंधी संक्षिप्त विवरण प्रस्तुत है।

भौतिकी का नोबेल पुरस्कार

राइनर वाइस, बैरी बैरिश और किप थोर्ने को वर्ष 2017 के भौतिकी के नोबेल पुरस्कार से सम्मानित किया गया है। इन तीनों अमेरिकी वैज्ञानिकों ने गुरुत्वीय तरंगों के अस्तित्व का पता लगाया और अल्बर्ट आइंस्टाइन के सदियों पुराने सिद्धांत को सच साबित किया। उनकी यह खोज गहन ब्रह्मांड के दरवाजे खोलती है। ये तीनों वैज्ञानिक लेजर इंटरफेरोमीटर ग्रैविटेशनल वेव ऑब्जर्वेटरी अर्थात् लीगो रिसर्च प्रोजेक्ट से जुड़े थे। लीगो भौतिकी का एक विशाल प्रयोग है, जिसका उद्देश्य गुरुत्वीय तरंगों के ब्लैक होल्स से टकराव का पता लगाना है। यह एमआईटी, काल्टेक तथा बहुत से अन्य संस्थानों की सम्मिलित परियोजना है। यह अमेरिका के नेशनल साइंस फाउण्डेशन द्वारा प्रायोजित है।

भौतिक विज्ञान में नोबेल पुरस्कार जीतने वाले ये तीनों वैज्ञानिक गुरूत्वाकर्षण तरंगों पर काम करते हैं जिसका उद्देश्य गुरूत्वाकर्षण तरंगों से न्यूट्रोन स्टार, ब्लैक होल्स और सुपरनोवा के बारे में जानकारी इकट्ठा करना है। गुरुत्वाकर्षण तरंगों की उपस्थिति को प्रमाणित करने में एक सदी लग गयी और 11 फ़रवरी 2016 को लीगो ऑब्ज़र्वेटरी के शोधकर्ताओं ने कहा है कि उन्होंने दो श्याम विवरों यानि ब्लैक होल की टक्कर से निकलने वाली गुरुत्वाकर्षण तरंगों का पता लगाया है। अब विश्वभर के वैज्ञानिकों को आइंस्टाइन की सापेक्षता के सिद्धांत (थिअरी ऑफ रिलेटिविटी) के प्रमाण मिल गए हैं। इसे अंतरिक्ष विज्ञान के क्षेत्र में बहुत बड़ी सफलता माना जा रहा है। गुरुत्वाकर्षण तरंगों की खोज से खगोल विज्ञान और भौतिक विज्ञान में खोज के नए दरवाजे खुलेंगे।