بخشی از ترجمه مقاله

عنوان فارسی مقاله :

الگوریتم کارآمد حریم خصوصی موقعیت مکانی برای خدمات و برنامه های کاربردی اینترنت اشیا(IoT)

عنوان انگلیسی مقاله :

Efficient Location Privacy Algorithm for Internet of Things (IoT) Services and Applications

توجه !

این فایل تنها قسمتی از ترجمه میباشد. برای تهیه مقاله ترجمه شده کامل با فرمت ورد (قابل ویرایش) همراه با نسخه انگلیسی مقاله، اینجا کلیک نمایید.

بخشی از ترجمه مقاله

8. Conclusion

In this paper, we first theoretically analyze the Dummy-Location selection (DLS) algorithm, which is the current approach to protect users' location privacy in LBS for IoT. Then, we discussed the current attack algorithm for DLS algorithm (ADLS) to identify the user's real location from chosen dummy locations generated by DLS algorithm. To efficiently preserve users' location privacy, we also propose a new Dummy Location Privacy (DLP) algorithm, by taking into account the equilibrium between the computational cost (i.e., time complexity) and the privacy requirements of users. Based on the obtained side information and the entropy metric, DLP algorithm greedily selects dummy locations to achieve the optimal privacy level of *k*-anonymity. We also analyze the security performance of the proposed DLP algorithm against potential attacks in the data-driven IoT service. Finally, we evaluate our DLP algorithm and ADLS algorithm by conducting extensive simulation experiments under various scenarios. The simulation results show that our ADLS algorithm has high probability of identifying the user real location from the dummy locations generated by DLS algorithm. Moreover, comparing with the DLS algorithm, our DLP algorithm has lower probability of revealing the user real location under the same attack, and can reduce the computational cost (i.e., time complexity) when providing same privacy level as the DLS algorithm. It will generate great impact for the data-driven IoT service to prevent attacks and preserve location privacy.

۸. نتیجه گیری

در این مقاله ما ابتدا به تجزیه و تحلیل نظری الگوریتم انتخاب موقعیت مکانی ساختگی (DLS) پرداختیم که رویکرد حاضر برای حراست از حریم خصوصی موقعیت مکانی کاربران در LBS برای IoT محسوب می گردد. سپس، ما درباره الگوریتم حمله حاضر برای الگوریتم DLS (ADLS) در شناسایی موقعیت مکانی واقعی کاربر از روی موقعیت مکانی ساختگی انتخابی حاصل از الگوریتم DLS بحث نمودیم. برای حفظ کارآمد حریم خصوصی موقعیت مکانی کاربران، ما نیز یک الگوریتم جدید حریم خصوصی موقعیت مکانی ساختگی (DLP) را با توجه به تعادل بین هزینه محاسباتی (یعنی پیچیدگی زمانی) و الزامات حریم خصوصی کاربران پیشنهاد نمودیم.
بر اساس اطلاعات جانبی حاصله و مقیاس آنتروپی، الگوریتم DLP به صورت حریضانه ای به انتخاب موقعیت مکانی ساختگی برای دستیابی به سطح حریم خصوصی بهینه k – ناشناختگی می پردازد. هم چنین ما عملکرد امنیتی الگوریتم DLP پیشنهادی را در برابر حملات بالقوه در خدمات IoT داده محور تجزیه و تحلیل نمودیم. نهایتاً، ما الگوریتم DLP و الگوریتم ADLS را با انجام آزمایشات شبیه سازی گسترده تحت سناریوهای مختلف ارزیابی نمودیم. نتایج شبیه سازی نشان می دهند که الگوریتم ADLS ما از احتمال بالایی در شناسایی موقعیت مکانی واقعی کاربر از روی موقعیت های مکانی ساختگی حاصل از الگوریتم DLS برخوردار است. افزون بر این، در مقایسه با الگوریتم DLS، الگوریتم DLP ما از احتمال کمتری برای آشکارسازی موقعیت مکانی واقعی کاربر تحت حمله مشابه برخوردار بوده، و می تواند هزینه محاسباتی (یعنی پیچیدگی زمانی) را در حین ارائه سطح حریم خصوصی مشابه با الگوریتم DLS کاهش دهد. این امر تاثیر زیادی برای خدمات IoT داده محور در پیشگیری از حملات و حفظ حریم خصوصی موقعیت مکانی در پی خواهد داشت.