IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 9, Issue 7, July 2021

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 7.542

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907021 |

Passport: A Secure and Private Location Proof Generation and Verification Framework

R.Jaisri[1], Dr.V.Vijayadeepa, M.Sc., MCA., M.Phil., Ph.D [2]

Research Scholar, Department of Computer Science, Muthayammal College of Arts and Science, Rasipuram, Tamilnadu, India[1]

Assistant Professor, Department of Computer Science, Muthayammal College of Arts and Science, Rasipuram, Tamilnadu, India[2]

ABSTRACT: Affording secure and competent big data aggregation methods is very attractive in the field of wireless sensor networks research. In concrete settings, the wireless sensor networks have been broadly functional, such as objective tracking and atmosphere remote monitoring. However, data can be simply compromised by a vast of attacks, such as data interception and data tampering, etc. In this paper, we mainly focus on data reliability protection; give an identity-based cumulative signature design with a designated verifier for wireless sensor networks. According to the advantage of cumulative signatures, our design not only can remain data reliability, but also can condense bandwidth and storage cost for wireless sensor networks. Furthermore, the security of our identity-based cumulative signature idea is strictly presented based on the computational Diffie-Hellman statement in random oracle form.

KEYWORDS: wireless sensor network, identity based, data aggregation, unforgeability, aggregate signature, coalition attack, designated verified

I. INTRODUCTION

The Location-Enabled mobile devices proliferate; location- based services are rapidly becoming immensely popular. Most of the current location-based services for mobile devices are based on users' current location. Users discover their locations and share them with a server. In turn, the server performs computation based on the location information and returns data/services to the users. In addition to users' current locations, there is an increased trend and incentive to prove/validate mobile users' past geographical locations. This opens a wide variety of new location-proof based mobile applications.described several such potential applications store wants to offer discounts to frequent customers Evidence of their repeated visits in the past to the store. A company which promotes green commuting and wellness may reward their employees who walk or bike to work. The company may encourage daily walking goals of some fixed number of miles. Employees need to prove their past commuting paths to the company along with time history. This helps the company in reducing the healthcare insurance rates and move towards sustainable lifestyle. On the battlefield, when a scout group is sent out to execute a mission, the commanding center may want every soldier to keep a copy of their location traces for investigation purpose after the mission. In digital universe grows in stunning speed which is produced by emerging new services, such as social network, cloud computing and internet of things. They are gathered by omnipresent wireless sensor networks, aerial sensory technologies, software logs, information-sensing mobile devices, microphones, cameras, etc. And the wireless sensor network is one of the highly anticipated key contributors of the big data in the future networks. Wireless sensor networks (WSNs), with a large number of cheap, small and highly constrained sensor nodes sense the physical world, has very broad application prospects both in military and civilian usage, including military target tracking and surveillance, animal habitats monitoring, biomedical health monitoring, critical facilities tracking. It can be used in some hazard environments, such as in nuclear power plants. Most of the current location-based services for mobile devices are based on users' current location. Users discover their locations and share them with a server. In turn, the server performs computation based on the location information and returns data/services to the users. In addition to users' current locations, there is an increased trend and incentive to prove/validate mobile users' past geographical locations. This opens a wide variety of new location-proof based mobile applications.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907021 |

II. METHODOLOGY

2.1 PROTOCOL

Our protocol consists of two primary phases: STP proof generation and STP claim and verification. Gives an overview of the two phases and the major communication steps involved. When a prover collects STP proofs from his/her co-located mobile devices, we say an STP proof collection event is started by the prover. An STP proof generation phase is the process of the prover getting an STP proof from one witness. Therefore, an STP proof collection event may consist of multiple STP proof generations. The prover finally stores the STP proofs collected in the mobile device. When a prover encounters a verifier (the frequency of such encounters is specific to the application scenarios) and intends to make a claim about his/her past STP to the verifier, the STP claim and verification phase takes place between the prover and the verifier. A part of the verification job has to be done by CA.Therefore, communication between the verifier and CA happens in the middle of the STP claim and verification phase. In, the two arrowed lines in red color represent the latter two stages of the Bussard-Bagga protocol. These stages require multiple interactions between the two involved parties, and thereby are represented by doubly arrowed lines. The preparation stage of the Bussard-Bagga protocol does not need to be executed for every STP proof generation and thus is not shown. Users could run the preparation stage before each STP proof collection event or pre-compute and store several sets of the bit commitments and primitives, and randomly choose one set.

2.2 SELFISH NODE

Our proposed entropy-based trust model guards from P-Wcollusion by giving lower trust values to STP proofs generated by common or repeating witnesses. It also serves as an incentive mechanism for users to generate STP proofs for strangers. In a generic case, peer mobile users may be selfish. They may choose to save their battery power over generating STP proofs for other users, particularly when they are strangers. Let us consider a simple case when User wants to generate his STP proofs from stranger.

III. COARSE GRAIN LOCATION

Trust computation becomes more reliable with increased number of users, hence choosing a coarser location level may be preferable for those services which seek higher reliability and trust but lower location granularity. We now show how STAMP can be used to collate STP proofs from witnesses from different locations to verify coarse grain location with higher trust.

IV. TRUSTED WITNESSES

STAMP is useful for a wide range of application where a centralized infrastructure (trusted wireless APs) is not available. The green commuting application we described scenario. In some scenarios, a trusted mobile or stationary user may be available or required. For example, a store which wants to give discounts to its frequent customers may have some trusted mobile users such as customer service agents who are amongst the crowd in the store. In the prior case, we have incognito trusted mobile users. For users going to a park, it was observed that there are frequent events when users find no co-located user to generate STP proofs. Thus, the authorities set up a trusted wireless AP to generate STP proofs for travelers. The exact location of such trusted wireless AP is known. In these scenarios, the prover can send all to CA or skip using CA since the proofs are already trusted. The first model fits well for incognito trusted mobile users while the other model serves well for wireless APs. Trusted Mobile Users: In first case, the trusted witness is not readily recognized by the prover. The prover will send original STP claim to the CA. The CA will recognize trusted witness among the many and also improve trust score for other witnesses, as an added incentive (recognizing their honest work).

V. CONCLUSION

This paper we have presented STAMP, which aims at providing security and privacy assurance to mobile users' proofs for their past location visits. STAMP relies on mobile devices in vicinity to mutually generate location proofs or uses wireless APs to generate location proofs. Integrity and non-transferability of location proofs and location privacy of users are the main design goals of STAMP. We have specifically dealt with two collusion scenarios: P-P collusion and P-W collusion. To protect against P-P collusions, we integrated the Bussard-Bagga distance bounding protocol into the design of STAMP. To detect P-W collusion, we proposed an entropy-based trust model to evaluate the trust level of claims of the past location visits. Our security analysis shows that STAMP achieves the security and

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 7.542 |

|| Volume 9, Issue 7, July 2021 ||

| DOI: 10.15680/IJIRCCE.2021.0907021 |

privacy objectives. Our implementation on Android smartphones indicates that low computational and storage resources are required to execute STAMP. Extensive simulation results show that our trust model is able to attain a high balanced accuracy with appropriate choices of system parameters Due to the limited resources of sensor nodes in terms of computation, memory and battery power, secure and energy save data aggregation methods should be designed in WSNs to reduce the energy cost of data collection, data processing and data transmission. In this paper, we present an ID-based aggregate signature scheme for WSNs, which can compress many signatures generated by sensor nodes into a short one, i.e., it can reduce the communication and storage cost. Moreover, we have proved that our IBAS scheme is secure in random oracle model based on the CDH assumption, and we also have proved that our aggregate signature can resist coalition attacks, that is to say the aggregate signature is valid if and only if every single signature used in the aggregation is valid. In our future work, we will focus on designing more efficient data

REFERENCES

[1] S. Saroiu and A. Wolman, "Enabling new mobile applications with location proofs," in *Proc. ACM HotMobile*, 2009, Art. no. 3.

[2] W. Luo and U. Hengartner, "VeriPlace: A privacy-aware location proof architecture," in *Proc. ACM GIS*, 2010, pp. 23–32.

[3] Z. Zhu and G. Cao, "Towards privacy-preserving and colluding-resistance in location proof updating system," *IEEE Trans. Mobile Comput.*, vol. 12, no. 1, pp. 51–64, Jan. 2011.

[4] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims," in *Proc. ACM WiSe*, 2003, pp. 1–10.

[5] R. Hasan and R. Burns, "Where have you been? secure location provenance for mobile devices," *CoRR* 2011.

[6] B. Davis, H. Chen, and M. Franklin, "Privacy preserving alibi systems," in *Proc. ACM ASIACCS*, 2012, pp. 34–35.

[7] I. Krontiris, F. Freiling, and T. Dimitriou, "Location privacy in urban sensing networks: Research challenges and directions," *IEEE Wireless Commun.*, vol. 17, no. 5, pp. 30–35, Oct. 2010.

[8] Y. Desmedt, "Major security problems with the 'unforgeable' (feige)- fiat-shamir proofs of identity and how to overcome them," in *Proc. SecuriCom*, 1988, pp. 15–17.

[9] L. Bussard and W. Bagga, "Distance-bounding proof of knowledge to avoid real-time attacks," in *Security and Privacy in the Age of Ubiquitous Computing*. New York, NY, USA: Springer, 2005.

[10] B. Waters and E. Felten, "Secure, private proofs of location," Department of Computer Science, Princeton University, Princeton, NJ, USA, Tech. Rep., 2003.

[11] C. Chen, C. Zhang, "Data-intensive applications, challenges, techniques and technologies: A survey on Big Data," *Information Sciences,* vol. 275, no. 11, pp. 314-347, 2014.

[12] D. Takaishi, H. Nishiyama, N. Kato and R. Miura, "Toward Energy Efficient Big Data Gathering in Densely Distributed Sensor Networks," *Emerging Topics in Computing IEEE Transactions on,* vol. 2, no. 3, pp.388-397, 2014.

[13] M.M.E.A. Mahmoud and X. Shen, "A cloud-based scheme for protecting source-location privacy against hotspot-locating attack in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 10, pp. 1805- 1818, 2012.

[14] I.F. Akyildiz, W. Su, Y. Sankarasubramaniam and E. Cayirci, "A survey on sensor networks," *IEEE Commun. Mag.*, vol. 40, no. 8, pp. 102-114, 2002.

[15] J. Yick, B. Mukherjee and D. Ghosal, "Analysis of a prediction-based mobility adaptive tracking algorithm," *in Proc. Broadband Networks, 2nd International Conference on, IEEE,* pp. 753-760, 2005.

[16] A. Mainwaring, J. Polastre, R. Szewczyk, D. Culler and J. Anderson, "Wireless Sensor Networks for Habitat Monitoring," *in Proc. WSNA'02*, Atlanta, Georgia, September, 2002.

[17] X. Lin, R. Lu, X. Shen, Y. Nemoto and N. Kato, "Sage: a strong privacypreserving scheme against global eavesdropping for ehealth systems," *Selected Areas in Communications, IEEE Journal on*, vol. 27, no. 4, pp. 365-378, 2009.

[18] R. Lu, X. Lin and X. Shen, (2013) "SPOC: A secure and privacypreserving opportunistic computing framework for mobile-healthcare emergency," *Parallel and Distributed Systems, IEEE Transactions on,* vol. 24, no. 3, pp. 614-624, 2013.

[19] C. Kim, G. Avoine, F. Koeune, F. Standaert, and O. Pereira, "The Swiss-knife RFID distance bounding protocol," in *Proc. ICISC*, 2009, pp. 98–115.

[20] H. Han *et al.*, "Senspeed: Sensing driving conditions to estimate vehicle speed in urban environments," in *Proc. IEEE INFOCOM*, Apr. 2014, pp. 727–735.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 7.542

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details