IJIRSET
International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 9, September 2022

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.118

9940 572 462 | 6381 907 438 | ijirset@gmail.com | www.ijirset.com

International Journal of Innovative Research in Science, Engineering and Technology (IJIRSET)

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109018 |

Survey of Network Intrusion Detection Methods from the Perspective of the Knowledge Discovery in Data Base Process

Ms.V.Thilagavathi[1], Dr. V. Vijayadeepa[2], M.Sc.,MCA.,M.Phil.,Ph.D.,

Research Scholar, Department of Computer Science, Muthayammal College of Arts and Science

Rasipuram, Tamilnadu, India

Head/ Department of Computer Application, Muthayammal College of Arts and Science

Rasipuram, Tamilnadu, India

ABSTRACT: The identification of community attacks on information and communication structures has been a focal point of the research community for years. Network intrusion detection is a complicated task which affords a large number of challenges. Many attacks presently go undetected, whilst more modern ones emerge due to the proliferation of linked devices and the evolution of verbal exchange generation. In this survey, we overview the strategies that have been implemented to gather community information with the motive of developing an intrusion detector, but contrary to previous evaluations in the area, we analyses them from the viewpoint of the Knowledge Discovery in Databases (KDD) method. In this paper, we present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. Our prototype implementation. 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: Big data, wireless sensor network, identity based, data aggregation, enforceability, aggregate signature, coalition attack, designated verified

I. INTRODUCTION

As 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. Customers must be able to show 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 big data era, digital universe grows in stunning speed which is produced by emerging new services, such as social network, cloud computing and internet of things. Big data 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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109018 |

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.

II. RELATED WORK

The concept of image inpainting was first introduced by Herve Debar , Marc Dacier , Andreas Wespi,[1] Intrusion-detection systems aim at detecting attacks against computer systems and networks, or against information systems in general, as it is difficult to provide provably secure information systems and maintain them in such a secure state for their entire lifetime and for every utilization. In this paper, we introduce a taxonomy of intrusion-detection systems that highlights the various aspects of this area. This taxonomy defines families of intrusion-detection systems according to their properties. Tingshan Huang, Harish Sethu and Nagarajan Kandasamy [2] Based on theoretical insights proved in this paper, we propose a new distance-based approach to dimensionality reduction motivated by the fact that the real-time structural differences between the covariance matrices of the observed and the normal traffic is more relevant to anomaly detection than the structure of the training data alone. P. Garcıa-Teodoroa, J. Dı´az-Verdejoa, G. Macia-Fernandeza, E. Va zquezb [3]This paper begins with a review of the most well-known anomaly-based intrusion detection techniques. Then, available platforms, systems under development and research projects in the area are presented. Finally, we outline the main challenges to be dealt with for the wide scale deployment of anomaly-based intrusion detectors, with special emphasis on assessment issues. Anna Sperotto, Gregor Schaffrath, Ramin Sadre, Cristian Morariu, Aiko Pras and Burkhard Stiller [4] Intrusion detection is an important area of research. Traditionally, the approach taken to find attacks is to inspect the contents of every packet. The paper provides a classification of attacks and defense techniques and shows how flow-based techniques can be used to detect scans, worms, Botnets and Denial of Service (DoS) attacks. Borja Molina Coronado, Usue Mori, Alexander Mendiburu and Jose Miguel-Alonso [5]As such, we discuss the techniques used for the collecion, preprocessing and transformation of the data, as well as the data mining and evaluation methods. We also present the characteristics and motivations behind the use of each of these techniques and propose more adequate and up-to-date taxonomies and definitions for intrusion detectors based on the terminology used in the area of data mining and KDD. Special importance is given to the evaluation procedures followed to assess the detectors, discussing their applicability in current, real networks. Monowar H. Bhuyan, D. K. Bhattacharyya, and J. K. Kalita [6] In this paper, we provide a structured and comprehensive overview of various facets of network anomaly detection so that a researcher can become quickly familiar with every aspect of network anomaly detection. We present attacks normally encountered by network intrusion detection systems. L. Buczak, Erhan Guven [7] Papers representing each method were identified, read, and summarized. Because data are so important in ML/DM approaches, some well-known cyber data sets used in ML/DM are described. The complexity of ML/DM algorithms is addressed, discussion of challenges for using ML/DM for cyber security is presented, and some recommendations on when to use a given method are provided.

III. METHODOLOGY

We present the Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. STAMP is designed for ad-hoc mobile users generating location proofs for each other in a distributed setting. However, it can easily accommodate trusted mobile users and wireless access points. STAMP ensures the integrity and non-transferability of the location proofs and protects users' privacy. A semi-trusted Certification Authority is used to distribute cryptographic keys as well as guard users against collusion by a light-weight entropy-based trust evaluation approach. 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.

IV.EXPERIMENTAL RESULTS

STP proof generation and STP claim and verification. The two phases and the major communication steps involved. When collects STP proofs from his/her co-located mobile devices, we say an STP proof collection event is started. An STP proof generation phase is the process of the getting an STP proof from one witness. Therefore, an STP

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

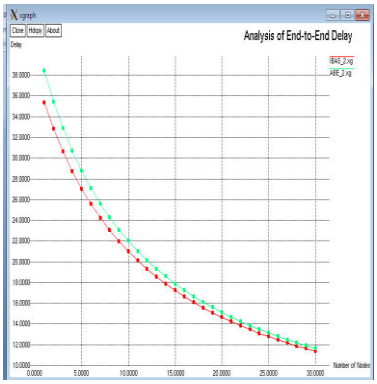
| DOI:10.15680/IJIRSET.2022.1109018 |

proof collection event may consist of multiple STP proof generations. The finally stores the STP proofs he/she collected in the mobile device. 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. 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. Data Mining also known as Knowledge Discovery in Databases, refers to the nontrivial extraction of implicit, previously unknown and potentially useful information from data stored in databases. Data Cleaning: Data cleaning is defined as removal of noisy and irrelevant data from collection. The Spatial-Temporal provenance Assurance with Mutual Proofs (STAMP) scheme. In contrast to most existing location proof systems which rely on infrastructure like wireless APs, STAMP is based on co-located mobile devices mutually generating location proofs for each other. This makes STAMP desirable for a wider range of applications. The exact location of such trusted wireless AP is known. In these scenarios, the 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.

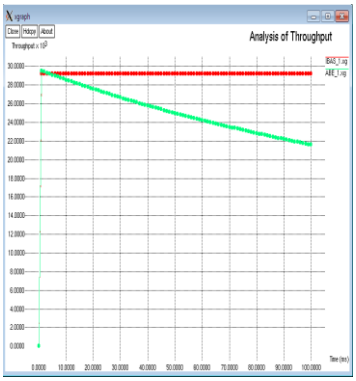
TABLE REPRESENTATION

Packet	Start	End	Values
Packet Size	1000	2000	1234
Transmission Speed	60	65	62
Node Strength	100	200	124
Mobility Range	250	500	258
Average Delay	5	15	6
Time Interval	5	8	7

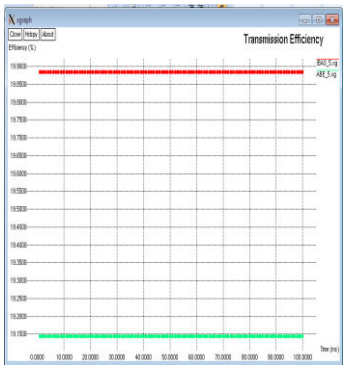
CHART FOR THE TABLE REPRESENTATION



(a)



(b)



(c)

VI. 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 privacy objectives. Our implementation on Android smart phones 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

| e-ISSN: 2319-8753, p-ISSN: 2320-6710| www.ijirset.com | Impact Factor: 8.118|

||Volume 11, Issue 9, September 2022||

| DOI:10.15680/IJIRSET.2022.1109018 |

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. 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.

BIOGRAPY

Dr.V.Vijayadeepa received her B.Sc degree from university of Madras and M.Sc degree from Periyar University. She has completed her M.Phil at Bharathidasan University. She has awared Ph.D by Anna University, Chennai. She is having 20 years of experience in collegiate teaching and She is the HoD of Department of Computer Application and Head of Student Progression in Muthayammal college of Arts and Science affiliated by Periyar University. Her main research interests include personalized Web search, Web Mining, Web information retrieval, data mining, and information systems.

Ms. V. Thilagavathi completed B.Sc (Computer Science) degree from Muthayammal memorial college of Arts & Science, Periyar University and M.Sc(Computer Science) degree from Muthayammal College of Arts & Science. Presently doing M.Phil Computer Science in Muthayammal College of Arts & Science, Periyar University.

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor: 8.118

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

Scan to save the contact details