WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

A Novel Secure Transmission of Secret Channel Encryption

Dr. R. Geetha [1], Mr. M. Santhosh [2], Ms. M. Ramani [3], Mr. B.Saran [4], Ms. G. Santhanapriya [5], Mr. S. Sangeeth [6]

[1] Associate Professor, Department of MCA, KSR College of Engineering, Tiruchengode, geethar@ksrce.ac.in,
[2, 3, 4, 5, 6] Student, Department of MCA, KSR College of Engineering, Tiruchengode,
santhoshmurugan890@gmail.com, ramanimurugan23@gmail.com, saranbalaji232@gmail.com, priyaganesan8448@gmail.com, sangeethnkl8481@gmail.com

ABSTRACT:

In this system, we present a best method for embedding provenance into the interpacket timing domain, which addresses the above mentioned problems and allows for the secure transmission of data's source for streaming (with a focus on sensor networks).Our approach can be thought of as a watermarking technique because the origin is concealed in another host medium. The problem of data degradation brought on by watermarking is avoided, however, because we integrate provenance over the interpacket delays (IPDs) as opposed to the sensor data itself. Using an ideal threshold-based technique that reduces the likelihood of provenance decoding mistakes, provenance is extracted by the data receiver. A detailed security study is used to determine how resilient the scheme is to external and internal attackers. This system demonstrates that our method can recover provenance up to a certain level in the presence of disruptions to the inter-packet timing features.

IPD, digital watermarking, safe transmission, data provenance and security.

1.INTRODUCTION

An unheard-of level of accessibility and redistribution for digital content has been made possible by the Internet's explosive expansion and related technologies. Enforcing data ownership in such a situation is a crucial requirement that calls for clear solutions that take into account technical, organizational, and legal factors. Digital image watermarking is a technique in which watermark data is embedded into a multimedia product and, later, is extracted from or detected in the watermarked product. These methods ensure tamper-resistance, authentication, content verification, and integration of the image.

With such methods, the data's owner is able to incorporate a barely noticeable watermark.

- Traditional security measures like encryption, digital signatures, and message authentication codes could be the basis of one potential solution to the issue of secure provenance for streaming (MAC).Each individual participating in the data processing would add their information to the data and sign it using a digital signature (or MAC)-based method to ensure validity. The usage of both encryption a method for secure document provenance based on incremental chained signatures could also be modified for sensor network application.. Due of provenance information's tendency to increase quickly and frequently reach sizes several orders of magnitude greater than the initial data, such approaches are inapplicable in sensor networks with limited resource availability. Hence, Such a trait would necessitatethe large transmission of provenance information along with data. Even after compaction, encryption, endorsement and MAC-based techniques are powerless to reduce this size. Hence, typical security methods use up a lot of bandwidth and reduce productivity and scalability.
- In our situation, several data sources often creates several packets; hence as well as sizable clusters of packets with quite similar origin. Here is another factor that might encourage the adoption of existing security techniques. In this situation, provenance can be sent in a few chosen packets with a low frequency using the privacy encryption/MAC/digital signature technologies. Such a strategy has the disadvantage that by looking at and examining every data packet, the attackers would be able to determine which packets included provenance.

1.2 OVERVIEW

The global spread of streaming applications has been tremendously aided by the Internet's growth, embedded devices, and sensor networks. The control of automated systems, location-based services, transaction records, sensor networks, and real-time financial analysis are a few examples. Such systems rely on many data sources, ranging from other systems to particular sensors, which are then handled by a number of intermediary agents. The relevance of data provenance to ensure the secure and reliable functioning of streaming applications is increased by the variety of data sources.

The history of ownership and actions taken with regard to the data is condensed by data provenance, which is regarded as a useful tool for assessing the reliability of the data. Recent studies on the provenance-based assessment of the reliability of sensor data, location data, and multi-hop networks show the importance of provenance in data streams. Take a battlefield surveillance system, for instance, which manages queries over the data it collects about enemy positions from several sensors placedwhile driving, aircraft, spacecraft, etc. In such a system, only data with a high degree of confidence may be accessed by mission-critical applications to ensure precise judgements. The management of provenance securely is given priority in this situation, making the assurance of data trustworthiness essential. The analysis of real-time data gathered from various sensors during process control activities also involves provenance.

2 SECRET CHANNEL ENCODING PROCESS

Finding Path

Take into account a network where there are a number of nodes and a number of directed links linking them. A sensor network comprises a group of small, powered devices, and a wireless or wired networked infrastructure. They record conditions in any number of environments including industrial facilities, farms, and hospitals.

Security Protection

security and protection system, any of various means or devices designed to guard persons and property against a broad range of hazards, including crime, fire, accidents, espionage, sabotage, subversion, and attack. Overt traffic can come at any time, resulting in an irregular pattern, whereas such a static encoding of data produces a fairly predictable behavior in the inter-packet delays.

Provenance Detection

In the context of sensor networks, we use the data provenance as details about the originating node and the nodes that processed/forwarded the data during its transmission. Formally, provenance detection propagates error-free information. The various provenance phases extraction areboth at the base station and at the sensor node, respectively.

Inter-Packet Delays (IPDS)

The sensor network allows data flows where source nodes regularly emit packets utilizing provenance encoding. Nodes might also accept data from additional nodes and passBS, it is. A node might transmit aggregated data value or sensed data generated by the routing node. The source node also timestamps the packet with the generation time. The provenance embedding and decoding procedures depend heavily on the packet timestamp. The communication channel is the inter-packet delays in chronological order (IPDs), and the signal transferred across it is the provenance.

Watermarking Technique

Digital Watermarking is use of a kind of marker covertly embedded in a digital media such as audio, video or image which enables us to know the source or owner of the copyright. This technique is used for tracing copyright infringement in social media and knowing the genuineness of the notes in the banking system. Our method can be thought of as a watermarking technique because provenance is concealed in another host media.

Data Transmission

Data transmission is the transfer of data from one digital device to another. This transfer occurs via point-to-point data streams or channels. These channels may previously have been in the form of copper wires but are now much more likely to be part of a wireless network.

A technique based on spread-spectrum watermarking that embeds provenance across the inter-packet delays was suggested for securely communicating provenance for data streams. We have implemented the widely used direct sequence spread spectrum (DSSS) approach, which enables several users to send packets simultaneously on the same frequency band by using different sequences.

2.1 Characteristics of Data Provenance:

It introduces the issue of safe provenance transfer for streaming data. It should be planned to integrate provenance in the inter-packet time domain using a watermarking-based method. A good threshold serves as the foundation for provenance technique. An experimental evaluation using fake data and a security analysis approach.

- Data Model: The phrase "data arrival" refers to data creation or receipt at a node. A node may operate as a routing node or transmit gathered information or transfer a value for gathered data calculated throughreadings from several detector. Each data packet includes the value and origin of an attribute. The source node additionally timestamps the packet with the creation time. To preserve its integrity and validity, we employ a message authentication code.

Data provenance is defined as details about the source node and the nodes that processed or passed the data throughout its transmission to the BS.

To Provide Confidentiality:

1. An attacker cannot discover provenance is present when looking at the temporal properties of the data flow it is unaware that derivationis being embedded across the IPDs. Even with knowledge of provenance embedding, the attacker is unable to obtain the provenance made up of trustworthy nodes.
2. The integrity of the provenance may only be accessed and verified by authorised individuals.

To Provide Integrity:

1. An attacker unsuccessfully adding authentic nodes pointing to the source offake data, whether operating alone or in concert with others.

2. The provenance of data created by benign nodes cannot be secretly altered by an attacker or a group of conspiring attackers.

To avoid forgery A legitimate provenance for a data packet cannot be argued to belong to another data packet by an attacker.Bringing freshness: It is impossible for an attacker to repeat recorded provenance and escape BS detection.

3. PROPOSED ARCHITECTURE

Safely communicating provenance for data streams is a novel challenge. We incorporate provenance over interpacket delays (IPDs) to prevent data deterioration brought on by watermarking. In digital work, watermarking embeds ownership information. The Watermark-based Approach has excellent Streaming Data Trustworthiness. A watermarking strategy can hide the provenance from an attacker. Digital watermarking ensures that the watermark will move with the material by including a hidden piece of information (watermark) into the content itself.

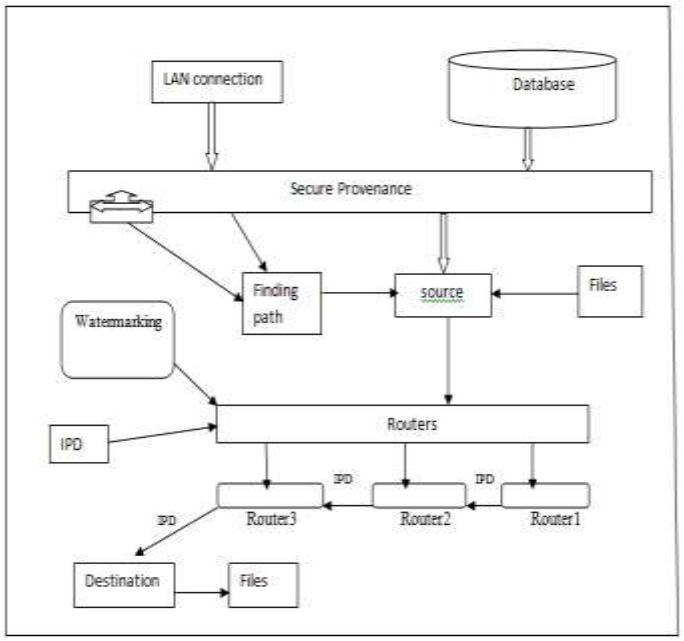

Fig.1 Block Diagram for Proposed Architecture

The information in one IPD is supported by the provenance dispersed over several IPDs. The provenance can be recovered throughout the decoding process to fend off different assaults. method using spread-spectrum watermarking to incorporate provenance over interpacket delays. The scheme's security characteristics enable it to withstand several Flow watermarking or a sensor network assaults. In the experimental findings demonstrate our plan is scalability and exceptional provenance retrieval resistance to a variety of assaults. We will later examine the viability of this method for large-sized provenance. By using several pseudonoise sequences, the widely used DSSS technology allows numerous users to communicate at once on the same frequency band.

4. OUR SCHEME

Provenance Detection

An attacker could wish to locate and retrieve a node's embedded provenance. To find and taint the network's active timing-based watermark.traffic, many techniques have been developed. Cabuk uses a hidden channel for network timing that sends single packet over a period of encoding duration a portionbefore going quiet. As overt traffic might come at any moment, a static encoding of the messages results in a highly regular

trend in the interpacket delays. Cabuk demonstrates how to locate a recurring pattern in the IPDs to locate the hidden channel. Peng and colleagues create an attack method to find the duplicate erased data.

Using packet timestamps at each intermediary host, the attacker attempts to deduce crucial watermarking parameters that are utilised to calculate watermark latency and the percentage of watermarked data. We provide a method to identify and automatically eliminate wide-area network flow watermarks (SSFW). Because the the rate of flow must be throttled by the encoder to a low level.

Digital Watermarking

Digital watermarking's main goal is to include hidden data about a piece of digital material into the content itself, guaranteeing that the watermark moves with the content. In order to watermark digitally, a watermark carrier domain must be chosen, and two complimentary procedures must be designed. an embedding procedure that produces the watermark carrier, the watermark message, and perhapsa key. a detection procedure that locates and extracts watermarks from incoming signals. As it can extract individual node IDs from the time-domain aggregated data, the detection process in our proposed system is more potent. watermarked, despite the fact that it resembles a watermarking technique.

Direct Sequence Spread Spectrum Technique

By using several pseudo noise sequences, the widely used DSSS technology enables numerous users to communicate concurrently on the same frequency band.

By treating the other signals as interference-like noise, the targeted receiver may recover the signal from the chosen user. This method is further separated into spreading and dispersing.

To create a spread signal, The PN code is multiplied by the data by the transmitter. A signal has been received. blend of the broadcast message and communication channel clash.

Fig.2 Connecting LANs for secure transmission

Fig.3. Selection of files for transmission

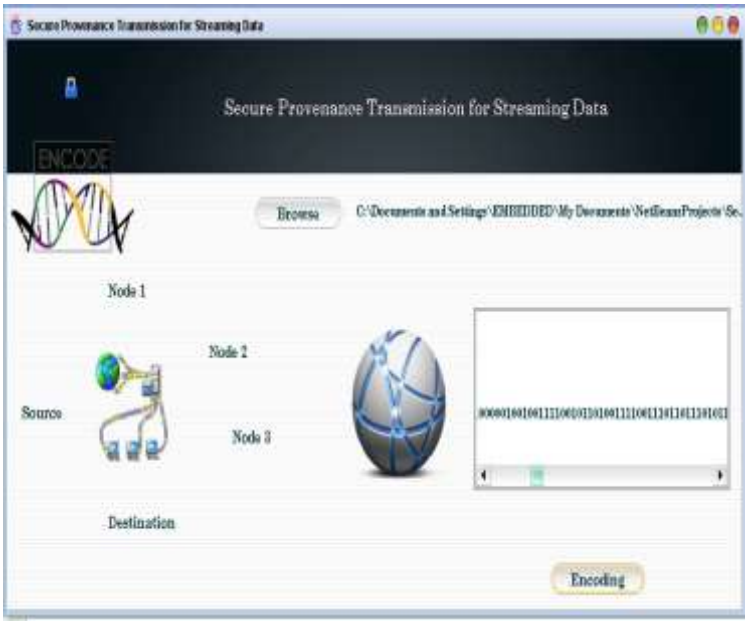

Fig.4.Encrypted files

5. CONCLUSION

By using an innovative watermarking approach to embed the provenance, it may be safely conveyed to the recipient side while guaranteeing its reliability. The scheme's security features enable it to withstand various sensor network or flow watermarking attacks. Examine the viability of this method for huge provenance. The data receiver extracts provenance using an ideal threshold-based approach that reduces the possibility of provenance decoding errors. A thorough security study is used to determine the scheme's resistance to both internal and external attackers. The proposed system demonstrate that our method can restore provenance up to a certain level against changes to the inter-packet timing features more though the provenance is safe, there are ways to make it more and more secure and more effectively for secure communication and reliability across the network. Since provenance is integrated via IPDs, its presence cannot be determined by looking at the time features of data flow.If the attacker is aware of provenance embedding, even then, it is unable to get the provenance made up of trustworthy nodes.

6. REFERENCES

[1].Berk V, Cybenko G, and Giani A, 2005, "Detection of Covert Channel Encoding in Network Packet Delays," technical report, Dartmouth College.

[2] Elson J and Estrin D, 2001, "Time Synchronization for Wireless Sensor Networks," Proc. Int'l Parallel and Distributed Processing Symp. (IPDPS), p. 186.

[3] Lim H and Moon Y , 2010, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. Workshop Data Management for Sensor Networks, pp. 2-7.

[4].Muniswamy-Reddy K.K, and Seltzer M, 2006 ,"Provenance-Aware Storage Systems," Proc. USENIX Ann. Technical Conf., p. 4.

[5]Ning P, Peng P,and Reeves D.S, 2006,"On the Secrecy of Timing-Based Active Watermarking Trace-Back Techniques," Proc. IEEE Symp. Security and Privacy (SP), pp. 334-349.

[6]Plale B ,and Simmhan Y.L, 2005,"A Survey of Data Provenance in E-Science," SIGMOD Record, vol. 34, pp. 31-36.

[7]Plale B, Vijayakumar N, 2006 "Towards Low Overhead Provenance Tracking in Near Real-Time Stream Filtering," Provenance and Annotation of Data, vol. 4145, pp. 46-54.

[8]Sakurai K , and, Syalim A, 2010 "Preserving Integrity and Confidentiality of a Directed Acyclic Graph Model of Provenance," Proc. Working Conf. Data and Applications Security and Privacy, pp. 311-318.