IJIRCCE

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

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 11, Issue 2, February 2023

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102017 |

Secure Transmission Discovery of Latency Secret Channel Encoder

MR.R.MOHANKUMAR, PRASANTH B

Assistant Professor, Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

Department of Computer Applications (MCA), K.S.R. College of Engineering (Autonomous), Tiruchengode, India

ABSTRACT: In this paper, we propose a novel approach to securely transmit provenance for streaming data (focusing on sensor network) by embedding provenance into the interpacket timing domain while addressing the above mentioned issues. As provenance is hidden in another host-medium, our solution can be conceptualized as watermarking technique. However, unlike traditional watermarking approaches, we embed provenance over the interpacket delays (IPDs) rather than in the sensor data themselves, hence avoiding the problem of data degradation due to watermarking. Provenance is extracted by the data receiver utilizing an optimal threshold-based mechanism which minimizes the probability of provenance decoding errors. The resiliency of the scheme against outside and inside attackers is established through an extensive security analysis. Experiments show that our technique can recover provenance up to a certain level against perturbations to inter-packet timing characteristics.

KEYWORDS: IPD, Digital watermarking, secure transmission, Data provenance

I.INTRODUCTION

The rapid growth of the Internet and related technologies has offered an unprecedented ability to access and redistribute digital contents. In such a context, enforcing data ownership is an important requirement, which requires articulated solutions, encompassing technical, organizational, and legal aspects. Although we are still far from such comprehensive solutions, in the last years, watermarking techniques have emerged as an important building block that plays a crucial role in addressing the ownership problem. Such techniques allow the owner of the data to embed an imperceptible watermark into the data.

A possible approach to the problem of secure provenance for streaming could be based on traditional security solutions like encryption, digital signature, and message authentication code (MAC). In a digital signature (or MAC)-based mechanism, each party involved in the data processing would append its information to data and sign it (or compute and attach the MAC) to ensure authenticity. In addition, encryption and an incremental chained signature based approach for secure document provenance could be adapted for use in sensor networks. However, such approaches are not applicable in resource constrained sensor networks, because provenance information tends to grow very fast, often becoming several magnitudes in size larger than the original data. Such a characteristic thus would force the transmission of a vast amount of provenance information along with data. Encryption/signature/ MAC-based mechanisms cannot help in reducing such size even after compaction. Hence, traditional security means incur significant bandwidth overhead and impact efficiency and scalability.

Another reason that could motivate the adoption of existing security mechanisms is that in our context each data source typically generates a lot of packets; thus there are large groups of packets that have the same provenance. In this context, the expensive encryption/MAC/digital signature mechanisms can be used with low frequency to send provenance in some selected packets. However, such an approach has the drawback that the attackers would be able to identify the provenance containing packets by observing and analyzing all the data packets. Upon detection, the attacker could then drop such packets and block the provenance transmission. Even if such attacks could be detected, there would be no way to recover the destroyed provenance. Data provenance is considered as an effective tool for evaluating data trustworthiness, since it summarizes the history of the ownership and the actions performed on the data. Recent research works on the provenance-based evaluation of the trustworthiness of sensor data location data and multihop network manifest the key contribution of provenance in data streams.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102017 |

1.2 OVERVIEW

The proliferation of the Internet, embedded systems, and sensor networks has greatly contributed to the wide development of streaming applications. Examples include real-time financial analysis, location-based services, transaction logs, sensor networks, control of automated systems. The data that drives such systems is produced by a variety of sources, ranging from other systems down to individual sensors and processed by multiple intermediate agents. This diversity of data sources accelerates the importance of data provenance to ensure secure and predictable operation of the streaming applications.

Data provenance is considered as an effective tool for evaluating data trustworthiness, since it summarizes the history of the ownership and the actions performed on the data. Recent research works on the provenance-based evaluation of the trustworthiness of sensor data location data and multi-hop network manifest the key contribution of provenance in data streams. As an example consider a battlefield surveillance system that gathers enemy locations from various sensors deployed in vehicles, air-crafts, satellites, etc., and manages queries over these data. Mission critical applications in such a system must access only high confidence data in order to guarantee accurate decisions. Thus, the assurance of data trustworthiness is crucial here, which prioritizes the secure management of provenance. Likewise, provenance plays a role in process control tasks that analyze the real-time data collected from different sensors.

2 SECRET CHANNEL ENCODING PROCESS

Finding Path

Consider a network, where is a set of nodes and is a set of directed links connecting the nodes. A sensor networks, are characterized by continuous data streaming from multiple sources and through intermediate processing by multiple aggregators. The above polynomials solvable special case with integer delays points out a heuristic solution for the general NP-complete problem with arbitrary Nodes.

Security Protection

This protection is one of the security protections. When this data is sending information source to destination it will be configured to start automatically. Such a static encoding of data leads to a highly regular behavior in the inter-packet delays, whereas overt traffic arrives anytime, resulting in an irregular pattern.

Provenance Detection

The context of sensor networks, we use the data provenance as information about the source node and the nodes that processed/forwarded the data throughout its transmission. Provenance detection is formally propagating error-free information. It is extract the stages of provenance encoding at a sensor node and decoding at the base station.

Inter-Packet Delays (IPDS)

The sensor network supports data flows where source nodes generate packet periodically using provenance encoding. A node may also receive data from other nodes in order to forward them towards the BS. While transmitting, a node may send the sensed data or pass an aggregated data value computed from routing node. The packet is also time stamped by the source node with the generation time. The packet timestamp is crucial for provenance embedding and decoding processes. The sequence of inter-packet delays (IPDs) is the communication channel and the provenance is the signal transmitted through it

Watermarking Technique

Though our proposed scheme resembles a watermarking technique, the detection process in our scheme is more powerful since it can extract individual node identities from the aggregated data watermarked in time domain. Thus, the use of the spread spectrum technique for watermarking provides strong security against different attacks. As provenance is hidden in another host-medium, our solution can be conceptualized as watermarking technique.

Data Transmission

A securely transmitting provenance for data streams proposed a spread-spectrum watermarking-based solution that embeds provenance over the inter-packet delays. We have adopted the direct sequence spread spectrum (DSSS) technique which is widely used for enabling multiple users to transmit packet simultaneously on the same frequency range by utilizing distinct sequences.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102017 |

2.1 Characteristics of Data Provenance :

The problem of secure Provenance transmission for streaming data is introduced.A watermarking based approach for embedding provenance in the inter-packet timing domain should be deigned.Technique for provenance is based on an optimal threshold.Security analysis approach and an experimental evaluation using synthetic data.

Data Model: The term data arrival with the meaning of data generation or receipt at a node. While transmitting, a node may send the sensed data or pass an aggregated data value computed from multiple sensors' readings, or act as a routing node. Each data packet contains an attribute value and provenance for this attribute. The packet is also timestamped by the source node with the generation time.We use a message authentication code to maintain its integrity and authenticity.

Definition of data provenance as information about the source node and the nodes that processed/forwarded the data throughout its
transmission towards the BS

To Provide Confidentiality:

1. If an attacker does not know that provenance is being embedded over the IPDs, it cannot detect the presence of provenance by observing the data flow timing characteristics. Even if the attacker is aware of provenance embedding, it cannot retrieve the provenance consisting of legitimate nodes.

2. Only authorized parties can access
and check the integrity of the provenance

To Provide Integrity:

1.An adversary, acting alone or colluding with others, cannot successfully add legitimate nodes to the provenance of fake data.

2. An attacker or a set of colluding attackers cannot undetectably add or remove nodes from the provenance of data generated by benign nodes
To prevent forgery: An adversary cannot claim that a valid provenance for a data packet belongs to a different data packet.
To Provide Freshness: An adversary cannot replay capturedprovenance, avoiding detection at the BS.

III.PROPOSED ARCHITECTURE

The novel problem of securely transmitting provenance for data streams. we embed provenance over the interpacket delays (IPDs) it avoids the problem of data degradation due to watermarking.Watermarking embeds ownership information in digital content.The trustworthiness of Streaming Data is high in the Watermark based approach. Watermarking scheme can make the provenance invisible to the attacker. Digital watermarking is to hide a secret information (watermark) related to a digital content within the content itself thereby ensuring the movement of the watermark along with the content

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102017 |

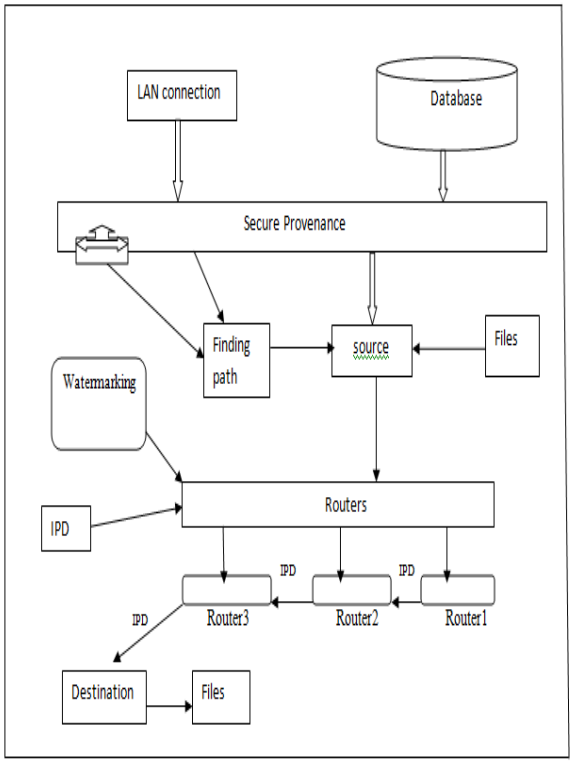

Fig.1.Block Diagram for Proposed Architecture

Provenance is spread over many IPDs such that the information present in one IPD. the decoding process can recover the provenance against various attacks. spread-spectrum watermarking-based solution that embeds provenance over the interpacket delays. The security features of the scheme make it able to survive against various sensor network or flow watermarking attacks.The experimental results show that our scheme is scalable and extremely resilient in provenance retrieval against various attacks. In future, we will investigate the feasibility of this technique for large sized provenance.DSSS technique which is widely used for enabling multiple users to transmit simultaneously on the same frequency range by utilizing distinct pseudonoise sequences

4 OUR SCHEME

Provenance Detection

An attacker might want to identify and extract the provenance embedded by a node. Several attacks have been devised to detect and corrupt the active timing-based watermark in network flows. Cabuk implements a covert network timing channel which transmits one packet in a time interval to encode the bit and stays silent for a bit. Such a static encoding of messages leads to a highly regular behavior in the interpacket delays, whereasovert traffic arrives anytime, resulting in an irregular pattern. Cabuk shows how to detect the covert channel by identifying a regular pattern in the IPDs. Peng et al. develop an attack technique to detect the duplicate removed data.

The attacker tries to infer important watermarking parameters step used to compute watermark delay and proportion of Watermarked using packet timestamps at each intermediate host and achieves the attack goals utilizing these parameters.we propose an approach to detect and autonomously remove spread spectrum flow watermarks (SSFW). Since the encoder needs to throttle the flow's throughput to a low value.

Digital Watermarking

The key idea of digital watermarking is to hide a secret information related to a digital content within the content itself thereby ensuring the movement of the watermark along with the content. Thus, digital watermarking involves the selection of a watermark carrier domain and the design of two complementary processes. An embedding

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102017 |

process that utilizes the watermarkcarrier, the watermark message and possibly a key to generate the watermarked data. A detector process that determines the existence of a watermark within the received signal and extracts it.

Though our proposed scheme resembles a watermarking technique the detection process in our scheme is more powerful since it can extract individual node identities from the aggregated data watermarked in time domain.

Direct Sequence Spread Spectrum Technique

DSSS technique which is widely used for enabling multiple users to transmit simultaneously on the same frequency range by utilizing distinct pseudonoise sequences . The intended receiver can extract the desired user's signal by regarding the other signals as noise-like interferences.This technique is futher divided as a Spreading and dispreading.The spreading is to transmitter multiplies the data with the PN code to produce spreaded signal.Despreading is received signal is a combination of the transmitted signal and noise in the communication channel.

Fig.2 Connecting LANs for secure transmission

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102017 |

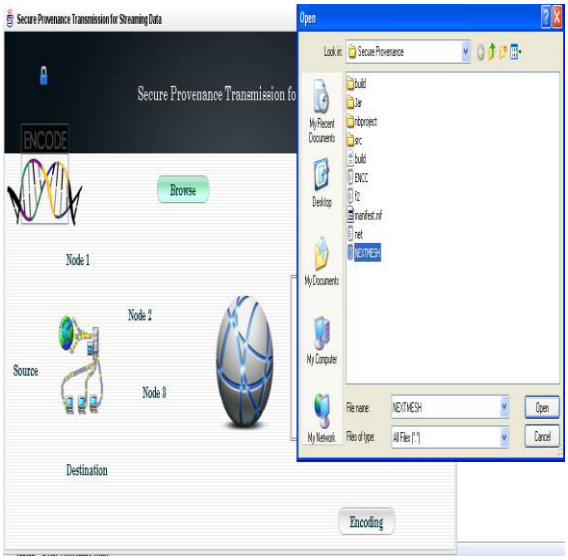

Fig.3. Selection of files for transmission

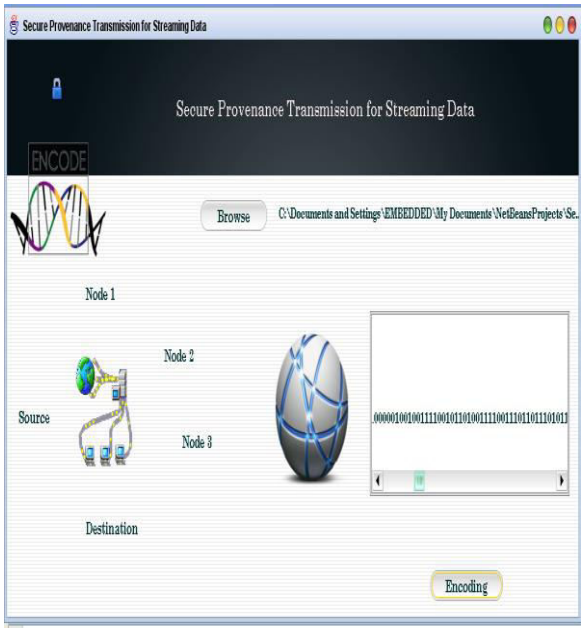

Fig.4. Encrypted files

V. CONCLUSION

The provenance can be securely transmitted to the receiver side by embedding it through advanced watermarking technique to ensure trustworthiness to the receiver side. The security features of the scheme make it able to survive against various sensor network or flow watermarking attacks. investigate the feasibility of this technique for large sized provenance. Provenance is extracted by the data receiver utilizing an optimal threshold-based mechanism which minimizes the probability of provenance decoding errors. The resiliency of the scheme against outside and inside attackers is established through an extensive security analysis. Experiments show that our technique can recover provenance up to a certain level against perturbations to inter-packet timing characteristics.Though the provenance is secure, we can find ways to provide more security to it and more efficiently for secure communication and trustworthiness across the network. provenance is being embedded over the IPDs, it cannot detect the presence of

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165|

|| Volume 11, Issue 2, February 2023 ||

| DOI: 10.15680/IJIRCCE.2023.1102017 |

provenance by observing the data flow timing characteristics. Even if the attacker is aware of provenance embedding, it cannot retrieve the provenance consisting of legitimate nodes.

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.

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

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