Secure and Provenance Transmission in Network

Briskilla.P
Department of Computer Science & Engineering
Christian College of Engineering & Technology
Oddanchatram, Dindigul, Tamilnadu-624619, India

Krishnadevi.R
Department of Computer Science & Engineering
Christian College of Engineering & Technology
Oddanchatram, Dindigul, Tamilnadu-624619, India

Kalarani.K
Department of Computer Science & Engineering
Christian College of Engineering & Technology
Oddanchatram, Dindigul, Tamilnadu-624619, India

Mr.A.JayaPrakash
ME.,(Ph. D)
Department of Computer Science & Engineering
Christian College of Engineering & Technology
Oddanchatram, Dindigul, Tamilnadu-624619, India

Abstract

Data provenance represents a key factor in evaluating the trustworthiness of sensor data. Provenance management for sensor networks introduces several challenging requirements, such as low energy and bandwidth consumption, efficient storage and secure transmission. To propose a novel lightweight scheme to securely transmit provenance for sensor data. The proposed technique relies on in-packet Bloom filters to encode provenance. We introduce efficient mechanisms for provenance verification and reconstruction at the base station. In addition, the secure provenance scheme to detect packet drop attacks staged by malicious data forwarding nodes. The results prove the effectiveness and efficiency of the lightweight secure provenance scheme in detecting packet forgery and loss attacks. It develop a Homomorphism Linear Authenticator (HLA) based public auditing architecture that allows the detector to verify the truthfulness of the packet drop information reported by nodes.

Keywords: WSN, ACF, HLA

I. Introduction

Networking is a group of two or more computers linked together by using WSN (Wireless Sensor Networks).In computer networking a, packet drop attack is a type of denial of service attack. In which a router this supposed to relay instead discards them. It investigates the problem of secure and efficient provenance transmission and processing for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes. To develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions. The main challenges in our mechanism lies in how to guarantee that the packet-loss bitmaps reported by individual nodes along the route are truthful, i.e., reflect the actual status of each packet transmission. Such truthfulness is essential for correct calculation of the correlation between lost packets; this can be achieved by some auditing. Public-auditing problem is constructed based on the homomorphism linear authenticator (HLA) cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients.

II. Related work

A. *Network Creation*

It create a multihop wireless sensor network, consisting of a number of sensor node and a base station that collects data from the network. The network is modeled as a graph that is communicating directly with each other. The Base station assigns each node a unique identifier node and a symmetric cryptographic key.

B. *Bloom filters process-Provenance Encoding*

Secure provenance technique can be used in conjunction with such work to obtain a complete solution that provides security for data provenance and data-provenance binding. It proposes a distributed mechanism to encode provenance at the nodes and a centralized algorithm to decode it at the BS. The technical core of our proposal is the notion of in-packet Bloom filter (iBF). Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance. We emphasize that our focus is on securely transmitting provenance to the Base station. Secure provenance technique can be used in conjunction with such work to obtain a complete solution that provides security for data provenance and data provenance binding.

C. *Provenances Encoding*

Extend the secure provenance encoding scheme to detect packet drop attacks and to identify malicious node(s).Assume the links on the path exhibit natural packet loss and several adversarial nodes may exist on the path. For simplicity, consider only linear data flow paths. Also, it do not address the issue of recovery once a malicious node is detected.

III. ARCHITECTURE

A. *Existing System*

Recent research highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures. The most of the related works preclude the ambiguity of the environment by assuming that malicious dropping is the only source of packet loss, so that there is no need to account for the impact of link errors. On the other hand, for the small number of works that differentiate between link errors and malicious packet drops, their detection algorithms usually require the number of maliciously-dropped packets to be significantly higher than link errors, in order to achieve acceptable detection accuracy. Following category, the second category targets the scenario where the number of maliciously dropped packets is significantly higher than that caused by link errors, but the impact of link errors is non-negligible.

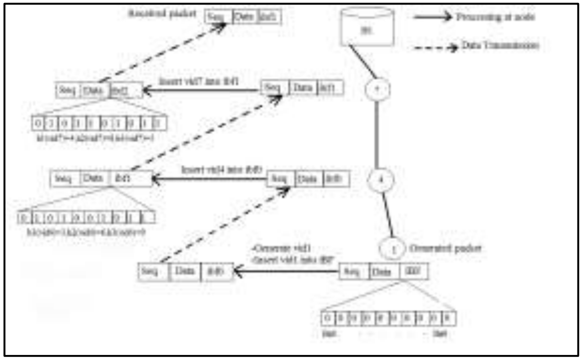

Fig. 1:

B. *Proposed System*

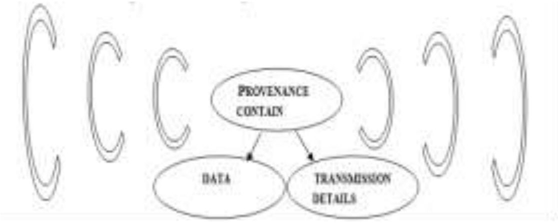

Fig. 2:

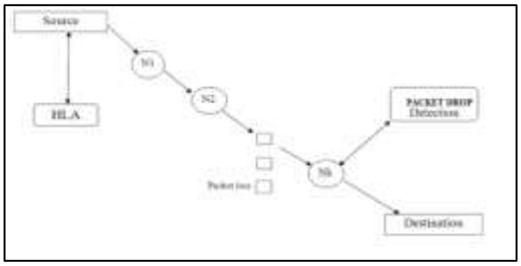

Fig. 3:

To investigate the problem of secure and efficient provenance transmission and processing for sensor networks, and we use provenance to detect packet loss attacks staged by malicious sensor nodes. To develop an accurate algorithm for detecting selective packet drops made by insider attackers. This algorithm also provides a truthful and publicly verifiable decision statistics as a proof to support the detection decision. The high detection accuracy is achieved by exploiting the correlations between the positions of lost packets, as calculated from the auto-correlation function (ACF) of the packet-loss bitmap–a bitmap describing the lost/received status of each packet in a sequence of consecutive packet transmissions.

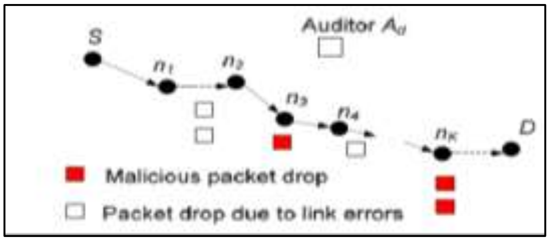

Fig. 4:

The main challenges in our mechanism lies in how to guarantee that the packet-loss bitmaps reported by individual nodes along the route are truthful, i.e., reflect the actual status of each packet transmission. Such truthfulness is essential for correct calculation of the correlation between lost packets; this can be achieved by some auditing.Public-auditing problem is constructed based on the homomorphism linear authenticator (HLA) cryptographic primitive, which is basically a signature scheme widely used in cloud computing and storage server systems to provide a proof of storage from the server to entrusting clients.

IV. Conclusion

The scheme ensures confidentiality, integrity and freshness of provenance. We extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. We developed an HLA-based public auditing architecture that ensures truthful packet-loss reporting by individual nodes.This architecture is collusion proof, requires relatively high computational capacity at the source node, but incurs low communication and storage overheads over the route.

References

[1] G.Ghinta, S.Sultana, “A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet DropAttacks in Wireless Sensor Networks”.
[2] A. Ghani and P. Nikander, “Secure In-Packet Bloom Filter Forwarding on the Netfpga,” Proc. European NetFPGA Developers Workshop, 2010.
[3] C.Rothenberg,C.Macapuna,M.Magalhaes, F.Verdi, A.Wiesmaier,In-Packet Bloom Filters: Design Networking Application, Computer Networks,vol.55,no,pp. 1364-1378,2011.
[4] S. Sultana, E. Bertino, and M. Shehab, “A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks,” Proc. Int’l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011.
[5] W. Zhou, M. Sherr, T. Tao, X. Li, B. Loo, and Y. Mao, “Efficient Querying and Maintenance of Network Provenance at Internet-Scale,” Proc. ACM SIGMOD Int’l Conf. Management of Data, pp. 615-626, 2010.