ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Detection of Provenance Forgery and Packet-Drop Attacks in Wireless Sensor Networks

Sunil S. Panchannavar, DR. R. Kanagavalli

M. Tech Student (Computer Network Engineering), Department of ISE, The Oxford College of Engineering, Visvesvaraya Technological University, Bangalore, India

Professor, Department of Information Science and Engineering, The Oxford College of Engineering, Visvesvaraya Technological University, Bangalore, India

ABSTRACT*:* Wireless sensor networks collect the data from the all nodes and which is used for the decision making purpose. Sometimes advisory node may introduce or compromise with the existing node so that the data can be easily altered. Data provenance verifies the sensor data. But some challenges are occurs while using provenance like space complexity, bandwidth consumption. In this paper a secure scheme is used to securely transmit provenance for sensor data. Here scheme uses only the bloom filter logic to encode and decode the data provenance and also energy efficient routing protocol for saving the energy of the network. Scheme extends the technique to find the packet drop attacks in the networks.

KEYWORDS*:* wireless sensor network, Provenance encoding, Provenance decoding, Data provenance, Security, Bloom filter.

I. INTRODUCTION

Wireless sensors used to aggregate the data from the environment like temperature, humidity, etc...Which are required for the decision making by base station. Only trustworthy information is considered in the decision making process. In a multi-hop sensor network, data provenance allows the BS to trace the source and forwarding path of an individual data packet. Provenance must be recorded for each packet, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes. Therefore, it is necessary to devise a light-weight provenance solution with low overhead. Furthermore, sensors often operate in an un-trusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance [1].

Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data [1]. Data encoding technique is used to encode the data provenance at sender node.

Data decoding algorithm which is used at the base station for verifying the data provenance i.e. the data is followed the same path or not, which is pre-decided by the sender node.

Packet loss minimizes the Packet Delivery Ratio. Packet loss can be caused by a number of factors including signal degradation over the network medium due to multi-path fading. Packet loss is possible in wireless sensor network. So that the intruders can be easily capture the data .Identifying the dropping packet and misbehaving activities are the most necessary measures for secure transmission in it. Without a certificate a node cannot participate in the transmission [2]. The technique also extended to find the data packet loss attack in the network.

Here the main goal is to encoding provenance and decoding mechanism that satisfies such security and performance needs. In provenance encoding each node on the path of a data packet securely attach provenance information within a

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information [1].

II.RELATED WORK

S. Roy, M. Conti, S. Setia, and S. Jajodia[1], In a large sensor network, in-network data aggregation significantly reduces the amount of communication and energy consumption. Recently, the research community has proposed a robust aggregation framework called synopsis diffusion which combines multipath routing schemes with duplicate-insensitive algorithms to accurately compute aggregates (e.g., predicate Count, Sum) in spite of message losses resulting from node and transmission failures. However, this aggregation framework does not address the problem of false subaggregate values contributed by compromised nodes resulting in large errors in the aggregate computed at the base station, which is the root node in the aggregation hierarchy. This is an important problem since sensor networks are highly vulnerable to node compromises due to the unattended nature of sensor nodes and the lack of tamper-resistant hardware.
T. Wolf [2], Capabilities-based networks present a fundamental shift in the security design of network architectures. Instead of permitting the transmission of packets from any source to any destination, routers deny forwarding by default. For a successful transmission, packets need to positively identify themselves and their permissions to the router. The analysis of the data path credentials data structure that et.al propose shows that as few as 128 bits are sufficient to reduce the probability of unauthorized traffic reaching its destination to a fraction of a percent.
S. Marti, T. J. Giuli, K. Lai, and M. Baker [3] et.al describes two techniques that improve throughput in an ad hoc network in the presence of nodes that agree to forward packets but fail to do so. To mitigate this problem, we propose categorizing nodes based upon their dynamically measured behavior. Technique uses a watchdog that identifies misbehaving nodes and a path rater that helps routing protocols avoid these nodes. Through simulation we evaluate watchdog and path rater using packet throughput, percentage of overhead (routing) transmissions, and the accuracy of misbehaving node detection.
Ramachandran [4] proposed Pedegree provenance scheme in which each packet is tagged with provenance data.
Tagger is deployed at each host which tags each packet with provenance data. Paper [4] used provenance data fortraffic classification and Arbiter is deployed at each hostwhich decides what to do with received packets having specific tags. Packet classification before Pedegree is mainly dependent on the IP addresses and port numbers but, after pedigree it has used tag information on the tags for packet classification. Pedegree scheme does not consider adversary network case and hence cannot deal with forgery attacks in the WSN.

Wenchao Zhou [5] et.al observed the need of securing the provenance information and proposed a scheme named, Secure Network provenance which gives proof for the state of the provenance data. Network operator can detect faulty nodes and also can assess the damage to network from such faulty nodes. Snoopy named SNP is proposed in paper and experimental results showed that Snoopy can prove state of provenance data in malicious WSN model. SNP scheme did not consider the limitations of WSN i.e. limited bandwidth, low battery and low memory.

Amril Syalim[6] Describes how to preserve integrity and confidentiality of a directed acyclic graph (DAG) model of provenance database. We show a method to preserve integrity by using digital signature where both of the provenance owner and the process executors (i.e. contributors) sign the nodes and the relationships between nodes in the provenance graph so that attacks to integrity can be detected by checking the signatures.

Nithya N. Vijayakumar[7] Proposed a data model and collection model for near real time provenance collection. And also define a system architecture for stream provenance tracking and motivate with a real-world application in meteorology forecasting.

III.SYSTEM ARCHITECTURE

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

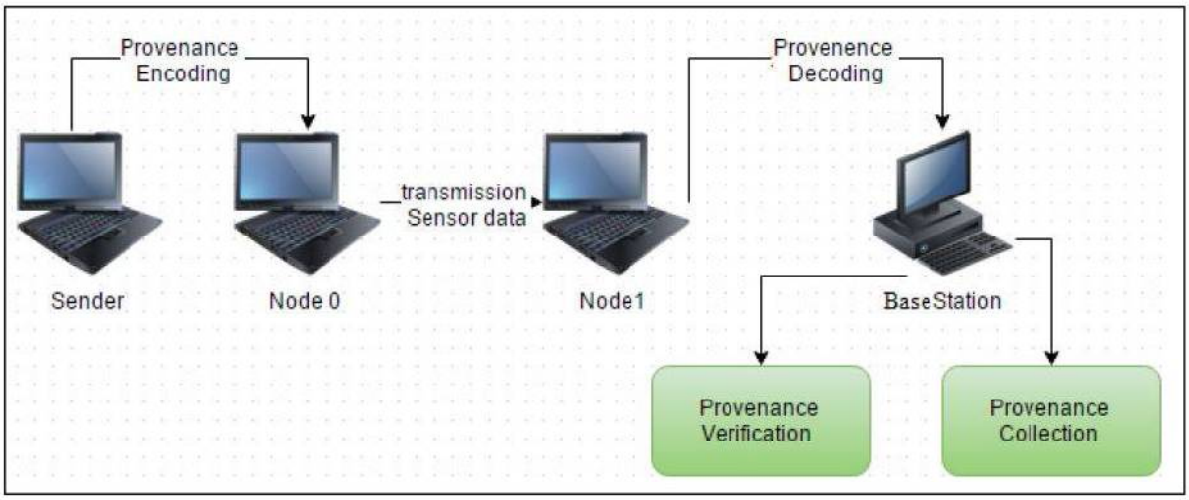

Figure 1.System architecture

Sensor networks are becoming increasingly popular in numerous application domains, such as cyber physical infrastructure systems, environmental monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at intermediate hops on their way to a base station that performs decision making. The Data provenance is an effective method to check data trustworthiness.

IV.IMPLEMENTATION

1. Data Packet Representation

To enable packet loss detection, a packet header must securely propagate the packet sequence number generated by the data source in the previous round. In addition, as in the basic scheme, the packet must be marked with a unique sequence number to facilitate per-packet provenance generation and verification. Thus, in the extended provenance scheme, any jth data packet contains (i) the unique packet sequence number (seq[j]), (ii) the previous packet sequence number (pSeq), (iii) a data value, and (iv) provenance.

2. Provenance Encoding

Secure provenance technique can be used to obtain a complete solution that provides security for data provenance and data-provenance binding. Scheme uses a distributed mechanism to encode Provenance at the nodes and a provenance decoding algorithm to decode it at the BS. The secure scheme uses in-packet Bloom filter (iBF). Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance. Here main focus is on securely transmitting provenance to the Base station. The provenance record of a node includes (i) the nodeID, and (ii) an acknowledgement of the lastly observed packet in the flow.

3. Provenance Decoding

When a Base station receives a data packet, upon receiving a packet, BS verifies its knowledge of provenance with that encoded in the packet. Not only the intermediate nodes, but also the BS stores and updates the latest packet sequence number for each dataflow. Upon receiving a packet, the BS retrieves the preceding packet sequence (pSeq) transmitted by the source node from the packet header, checks the last packet sequence for the flow from its storage (pSeqb), and utilizes these two sequences in the process of provenance verification and collection.

4.Detecting Packet Drop Attacks

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

The provenance encoding extend scheme to detect packet drop attacks in the network and also to identify malicious node(s) in the network . It assumes the links on the path exhibit natural packet loss and several adversarial nodes may exist on the path. For simplicity, It consider only linear data flow paths. Also, It do not address the issue of recovery once a malicious node is detected. Existing techniques that are orthogonal to our detection scheme can be used, which may initiate multipath routing or build a dissemination tree around the compromised nodes. For a data packet, the provenance record generated by a node will now consist of the node ID and an acknowledgement in the form of a sequence number of the lastly seen (processed/forwarded) packet belonging to that data flow. If there is an intermediate packet drop, some nodes on the path do not receive the packet. Hence, during the next round of packet transmission, there will be a mismatch between the acknowledgements generated from different nodes on the path. This fact is used to detect the packet drop attack and to localize the malicious node.

V. RESULTS

Here ns2 simulator is used to test the provenance technique. We considered the network of 40 nodes. First, we look At how effective the secure encoding scheme is in detecting provenance forgery and also the accuracy of the method for detecting packet loss. Finally we measure the energy consumption of provenance.

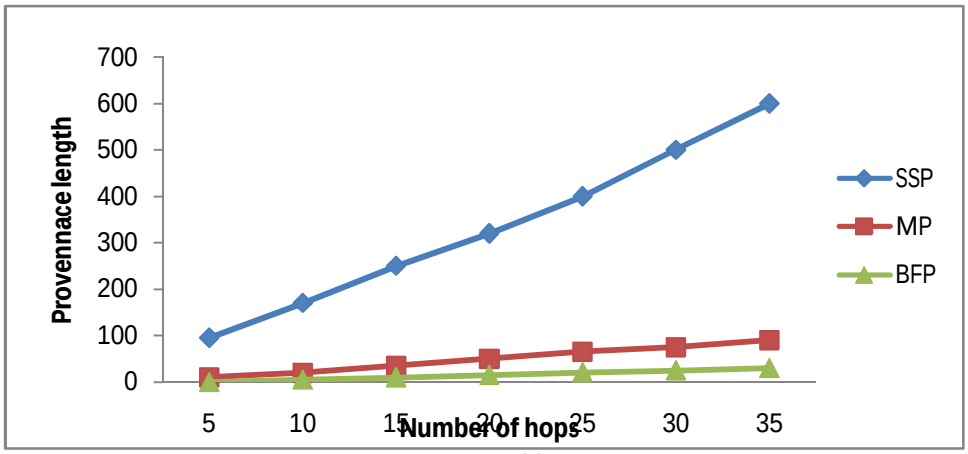

Fig 2(a)

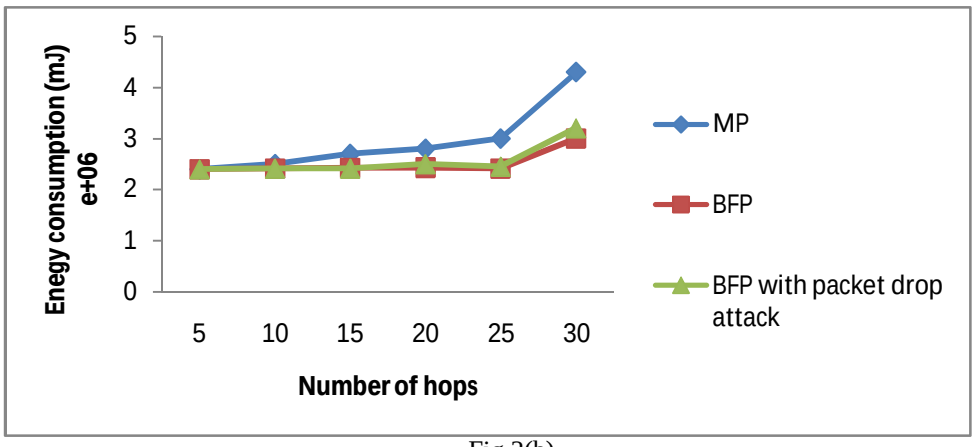

Fig 2(b)

ISSN(Online) : 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 4, April 2016

Compares SSP, MP and provenance mechanism in terms of bytes required to transmit data provenance. The provenance length in SSP and MP increases linearly with the path length. Compares SSP, MP and our provenance mechanism in terms of bytes required to transmit provenance. The provenance Length in SSP and MP increases linearly with the path length. The BF size increases with the expected number of elements to be inserted, the increasing rate is not linear. In this scheme 30 bytes is enough to transmit the data provenance for 35 hops path .Fig 2(b) measure the energy consumption for both the basic provenance scheme and the extended scheme for packet drop detection, while varying hop counts.

VI.CONCLUSION AND FUTURE WORKS

In this paper, we noted the problem of securely transmitting provenance for sensor networks, and used the provenance encoding and decoding scheme based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance. Here scheme extended to in-corporate data-provenance binding, and to include packet sequence information that supports detection of packet loss attacks. In future work, we plan to implement a real system with black hole attack and try to avoid the black hole attack.

REFERENCES

[1] Salmin Sultana,Gabriel Ghinita, and Mohamed Shehab, Member" A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks" Member, IEEE, Elisa Bertino, Fellow, IEEE, , IEEE [1]H. Lim, Y. Moon, and E. Bertino, "Provenance-based trustworthiness assessment in sensor networks," in Proc. of Data Management for Sensor Networks, 2010, pp. 2–7.
[2] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure network provenance," in Proc. of ACM SOSP, 2011, pp. 295–310.
[3] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure Data Aggregation in Wireless Sensor Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 3, pp. 1040-1052, June 2012.
[4] T. Wolf, "Data Path Credentials for High-Performance Capabilities- Based Networks," Proc. ACM/IEEE Symp. Architectures for Networking and Comm. Systems, pp. 129-130, 2008.
[5] S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. Int'l Conf. Mobile Computing and Networking, pp. 255-265, 2000.
[6] A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster, "Packets with Provenance," Technical Report GT-CS-08-02, Georgia Tech, 2008.
[7] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure Network Provenance," Proc. ACMSOSP, pp. 295-310, 2011.
[8] 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.
[9] N. Vijayakumar and B. Plale, "Towards Low Overhead Provenance Tracking in Near Real-Time Stream Filtering," Proc. Int'l Conf. Provenance and Annotation of Data (IPAW), pp. 46-54, 2006.
[10] A. Syalim, T. Nishide, and K. Sakurai, "Preserving Integrity and Confidentiality of a Directed Acyclic Graph Model of Provenance," Proc. Working Conf. Data and Applications Security and Privacy, pp. 311-318, 2010.
[11] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proc. Seventh Int'l Workshop Data Management for Sensor Networks, pp. 2-7, 2010.
[12] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data Derivation," Proc. Conf. Scientific and Statistical Database Management, pp. 37-46, 2002.
[13] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-Aware Storage systems," Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.
[14] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMODRecord, vol. 34, pp. 31-36, 2005.
[15] R. Hasan, R. Sion, and M. Winslett, "The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance," Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.