A SURVEY ON ENHANCED MODEL FOR IDENTIFYING PROVENANCE DUPLICATION AND PACKET DROP ATTACKS USING IN-PACKET BLOOM FILTERS

Deepak V s[1], Ranjitha U N s[2]

[1] *M.tech, Computer Science and Engineering, REVA ITM, Bangalore, India*

[2] *Professor, REVAITM, Bangalore, India*

Abstract -The large number of applications are working in large scale wireless sensor networks. In decision making these huge amount of data produced are used and these information is passed through multiple nodes along with many nodes that collects huge amount of information. Since the data collected is too large data integrity, security and trustworthiness plays an important role. The data provenance provides trustworthiness in sensor networks. Provenance management mainly requires minimum energy, minimum bandwidth consumption, proper storage and transmission. This method also uses bloom filter along with the data packets and also very good mechanisms for provenance checking and validation purposes at the base station

INTRODUCTION

The sensor networks are used in many applications such as healthcare's, weather fore casting, power grids, environmental monitoring etc. From these application domains the data is passed through network at intermediate nodes to base station. The huge amount of data information enforces the trustworthiness of data gathered. So in this paper they uses provenance security solution.

In this paper they uses distributed mechanism in order to provide provenance at the nodes which is called as in packet Bloom Filter (iBF) and it will work as decoding algorithm at the base station.

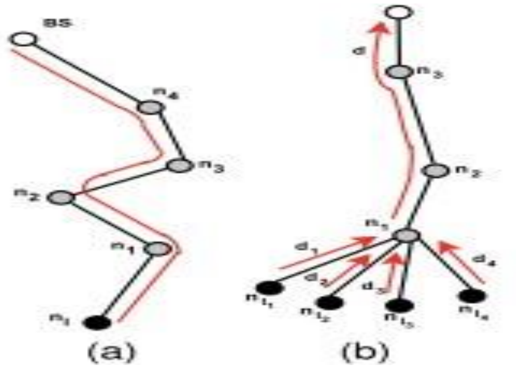

Fig 1.1 Provenancegraph for sensor network

The main aim of this scheme is to transfer provenance with the data to base station securely. The previous existing approaches are normally using two separate transmission channels for data packets and provenance. But in this technique they are using only a single channel for both data packets and provenance. Also previous methods are using digital signature and cryptography technique but in this process they are using message authentication code (MAC) and Bloom filter (BF) techniques. In this process the main three security objectives are integrity, confidentiality and freshness of provenance. For packet acknowledgement they uses provenance encoding. By using this technique they can find out the packet drops easily in the packet transmission.

I. RELATED WORK

There are many papers and techniques used for provenance methods, some of them are discussed below.

A. Packets with provenance (2008)

This paper was proposed by A. Ramachandran et al [1]. This paper provides provenance for data items in the form of packets tags which stores the history of all nodes. But this model assumes that environment must be trustworthy which is not possible all the time. In this technique they contains two components, they are a trusted tagger and an arbiter.

B. Provenance based trustworthiness assessment in sensor networks (2010)

This method is proposed by Bertino et al [2] on the multi hop network for provenance based data trustworthiness. In this method they used provenance as well as their values. This method takes both information and path correlation for evaluation. This method makes use of both provenance and its value.

C. Secure network provenance (2011)

This model was proposed by Wenchao Zhou et al [3]. Secure network provenance extends network provenance to adversarial environments. In this method we assumes every fault nodes behave arbitrarily. This covers wide range of mis -behaviour and faults. This technique works in a completely untrusted environment. Actually these systems are network provenance systems. So this method is not optimized for the resource constrained sensor networks.

D. Provenance transmission for streaming data (2013)

In 2012 Salmin sultana et all [4] are already worked on the provenance technology. They have used water marking method in this process. In this technique they embed provenance over the inter-packet delays rather than the sensor data. So it reduces the probability of error in provenance decoding. But amount of provenance grow very fast and transmission of this huge amount of provenance information along with data will causes bandwidth overhead and low efficiency and scalability.

E. Provenance using arithmetic coding (2014)

This model was proposed by Syed Rafiul Hussain et al [5]. In wireless sensor networks the provenance data increases as data passed from source to base station. So increase in the data provenance size slowdowns the performance. Hence this technique uses compression of data provenance. Here number of hops are not directly proportional to provenance size.

II. PROPOSED SYSTEM

In proposed system they provides a most efficient provenance technique which is used to detect the loss of packets by malicious sensor nodes. This model also provides a provenance encoding method in which each node along with the path of data packet, carries provenance information in a bloom filter. The Base Station receives the packets and it verifies the provenance information. In this model, Bloom filter (BF) and Message authentication code (MAC) techniques were used, which are of fixed size data structures. Since bandwidth is the main constraint in wireless sensor networks, Bloom filters are very useful and it gives very less error rates.

REFERENCES

[1] A. Ramachandran, K. Bhandankar, M. Tariq, andN.Feamster,“Packets with Provenance,” Technical Report GT-CS-08- 02, Georgia Tech, 2008. S. Sultana, M. Shehab, and E. Bertino, “Secure Provenance Transmissionfor Streaming Data,” IEEE Trans. Knowledge and Data Eng.,vol. 25, no. 8, pp. 18 90-1903, Aug. 2013

[2] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B., and M. Sherr,“Secure Network Provenance,” Proc. ACMSOSP, pp. 295310, 2011.

[3] S. Sultana, M. Shehab, and E. Bertino, “Secure Provenance Transmissionfor Streaming Data,” IEEE Trans. Knowledge and Data Eng.,vol. 25, no. 8, pp. 1890-1903, Aug. 2013.

[4] 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.

[5] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, “Provenance-Aware Storage systems,” Proc. USENIX Ann. Technical Conf., pp. 4-4, 2006.

[6] Y. Simmhan, B. Plale, and D. Gannon, “A Survey of Data Provenance in E-Science,” ACMSIGMOD Record, vol. 34, pp. 3136, 2005.

[7] C. Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wiesmaier, “In-Packet Bloom Filters: Design and Networking Applications,” Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011