A Secure and Efficient Framework for Data Transmission in Wireless Sensor Networks

Prof.Ananthanagu.U[1], Rekha.F.P[2]

Assistant Professor, Department of Computer Science and Engineering, AMCEC, Bangalore[1] , Karnataka, India

M-Tech Scholar, Department of Computer Science and Engineering, AMCEC, Bangalore[2], Karnataka, India

---***---

Abstract - *Large scale sensor networks are applied in various applications and the information which they collect are used in decision making for complicated infrastructure. Information combined from various sources through intermediate nodes that aggregate data. A harmful adversary may add extra nodes in network hence, persuading data reliable is critical for accurate decision making. Information provenance represents a key factor in evaluating reliable of sensor data. Provenance management for sensor networks introduces many challenging requirements like low in energy consumption and bandwidth consumption, storage efficiency and safe transmission. In this paper we introduce a single channel technique to secure transmit provenance for sensor data. The proposed technique relates on in-packet Bloom filters for encoding the provenance. We propose an effective mechanism for provenance construction and verification at base station. In additional, extending the safe provenance scheme with functionality to identify the packet drop attacks mount by harmful data forwarding nodes. Evaluate the introduced technique by both experimentally and analytically and the results prove the efficient and effective of low weight safe provenance technique scheme in identifying packet drop attacks and packet modifier.*

***Key Words*: Security, Provenance, Sensor Networks, Bloom Filter, Encoding, Decoding**

1. INTRODUCTION

Wireless Sensor networks are used in various applications domain like infrastructure of cyber physical systems, power grid etc.Information which gives at a more number of sensor node sources and organised in-network at intermediate hops on the way to a sink node where sink or base station performs decision making. The different form of data sources creates the require to persuade the reliable of data, like that only reliable data is observed in the process of decision making. Information provenance is an efficient method to evaluate reliable information, since it outlines the history of possession and the actions performed on data. The use of unreliable data may results in sudden failures like SCADA systems. We identify the problem of efficient and secure provenance transmitting and processing for sensor networks and we detect loss of packets which mount by harmful sensor nodes.

In a multi-hop sensor network, information provenance allows sink node to trace the source node and moving path of a single data packet. Provenance should be recorded for every packet, but essential challenges occurs because to the tight storage, bandwidth and energy of sensor nodes. Hence, it is required to mention security requirements like confidentiality, integrity, freshness of provenance. Our main aim is to designing a provenance encoding and decoding mechanism which satisfies such safe and performance .Here we introduce a provenance encoding method where each single node on path of data packet safely insert provenance data within a Bloom filter which is transmitted with the information. On receiving the packet, the sink node abstract and checks the provenance encoding scheme which allows the sink node to identify when a packet is dropped by a harmful node. We use only a single channel for both data and provenance and also we use only Message Authentication Code scheme and Bloom Filter Scheme. Bloom filter which are constant size data structure that represents provenance. It also makes effective usage of bandwidth and also results less error in practice.

Our certain benefactions are:

- We design the problem of safe provenance transmission sensor networks, and detect the challenges specific to this context.
- In packet BF provenance encoding scheme is proposed.
- For provenance decoding and verification at the base station we design efficient techniques.
- Safe provenance encoding scheme is extended and for detecting packet drop attacks devise an effective mechanism that are staged by harmful forwarding sensor nodes.
- Security analysis and performance evaluation of the proposed packet drop detection mechanism and provenance encoding scheme are performed in detail.

2. Related Work

Ramachandran [1] proposed Pedigree provenance scheme in which every packet is added with provenance information. Tagger is delivered at every host which add each packet with provenance information.

Wenchao Zhou [2] et.al identified the necessary of securing the provenance data and Secure Network provenance is proposed which gives evidence for the state of provenance information .Network operator identifies faulty nodes and it also determine the failure to network from such faulty nodes.SNP Snoopy name which is proposed in paper and Snoopy can prove state of provenance information in Harmful Wireless sensor Network model this can be showed in experimental results. Limitations of WSN did not consider by the SNP scheme.

Paper [3] addressed the necessity to identify source data which is transferred over the internet and introduced the scheme which gives effective confidentiality and also integrity of provenance data. Proposed scheme gives hold over the visibility of provenance data and assure no one can alter the data provenance without identification .Through encryption confidentiality and integrity is achieved.

Paper [4] Introduced a mechanisms where sensor data is aggregate with its provenance data rapidly and provenance data can be recovered from this tagged data. Special use of this scheme is that, provenance data is inserted in to actual sensor data. In any of the way also the security to provenance data does not provide by proposed system.

Paper [5] Narrate the design of the BF data structure and its efficiency .When information is encoded in to Bloom Filter, set of Hash function are used. Information which has to be encoded is hashed using hash functions. The hash function outcome will be in integer values. Main intention of using Bloom Filter is to check the subscribers of element. This paper mainly discussed about the bloom filter's potential network applications.

Paper [6] For Network management network accountability and failure analysis is essential. It also outlines the necessity of network provenance. Proposed ExSPAN provenance systems in distributed environment .To prove the state of network ExSPAN used provenance data. System is generic and extensible that is showed by experimental results. Safety of the provenance data is also not considered by this scheme.

Paper [7]To safe a directed acyclic graph of the data provenance proposed a method. By checking the signatures provenance information graph and integrity is validated.

3. EXISTING SYSTEM

The present research emphasize that the key contribution of provenance in systems, where the use of non reliable information which may lead to the disastrous failures for example SCADA systems. SCADA is Supervisory Control and Data Acquisition.

Although provenance modelling, collection and querying have been studied extensively for workflows and curate databases, provenance in Sensor Networks has not been properly addressed.

Disadvantages:

- Intensively use of Cryptography and digital signatures by the traditional provenance security solutions.
- Append-based data structure to store provenance, which leading to prohibitive costs which they are employed.
- Existing research employs separate transmission channel for data and separate transmission channel for provenance.

4. PROPOSED SYSTEM

We look in to problem of safe and effective provenance transmission and also processing for sensor networks, to observe packet drop attacks staged by harmful sensor nodes we use provenance. Our main aim is to design provenance encoding and provenance decoding mechanisms which satisfies the performance and also security needs. We propose a provenance encoding scheme where each node in the network on the path of packet data safely inserts provenance data within a Bloom Filter which is transmitted along with the information .we also devise an extension of the provenance encoding strategy that allows the sink node to identify if a packet loss attacks was mount by a harmful nodes.

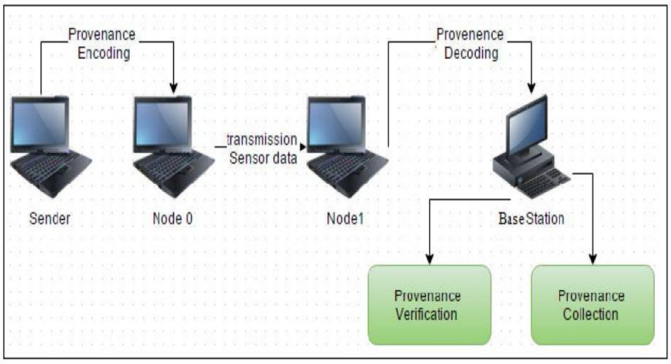

Fig 3 System Architecture

Advantages:

- Fast MAC and BF are only used .Bloom filter where it represents provenance they are fixed size data structures.
- We devise the problem of safe provenance transmission in sensor networks.
- In-packet Bloom filter encoding strategy is proposed.
- For provenance decoding and verification at sink node efficient techniques are designed.
- Secure provenance encoding scheme are extended and the packet loss attacks which are mount by malicious nodes are devised by a mechanism.
- Security analysis and evaluation of performance of the proposed provenance encoding scheme and also packet drop identification mechanisms are in detail performed.
- For transmission of both provenance and data, requires only single channel.

5. CONCLUSION AND FUTURE WORK

Securely transmitting provenance for sensor networks, and proposed a single channel for transmission of both data and provenance. Based on bloom filter provenance encoding and decoding scheme are proposed. The scheme protects confidentiality, integrity and freshness of provenance. To consolidate information provenance binding and to include packet sequence data that helps in identification of packet drop attacks are extended the scheme. The proposed scheme is efficient and scalable that is showed by the experimental and analytical evaluation results. In the future work intent to execute a real system prototype of our secure provenance strategy and also to raise the precision of packet drop identification especially in the case of numerous successive harmful sensor nodes.

REFERENCES

[1] S. Roy, M. Conti, S. Setia, and S. Jajodia, "Secure data aggregation in wireless sensor networks," IEEE Transactions on Information Forensics and Security, vol. 7, no. 3, pp. 1040–1052, 2012

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A virtual data system for representing, querying, and automating data derivation," in Proc.of the Conf. Scientific and Statistical Database Management, 2002, pp. 37–46.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Provenance-aware storage systems," in Proc. of the USENIX Annual TechnicalConf., 2006, pp. 4–4.

[4] Y. Simmhan, B. Plale, and D. Gannon, "A survey of data provenance in e-science," SIGMOD Record, vol. 34, pp. 31–36, 2005.

[5] R. Hasan, R. Sion, and M. Winslett, "The case of the fake picasso: Preventing history forgery with secure provenance," in Proc. Of FAST, 2009,pp. 1–14.

[6] S. Madden, J. Franklin, J. Hellerstein, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," SIGOPS Operating Systems Review, no. SI, Dec. 2002.

[7] A. Kirsch and M. Mitzenmacher, "Distance-sensitive bloom filters," in Proc. of the Workshop on Algorithm Engineering and Experiments, 2006.

[8] A. Kirsch and M. Mitzenmacher, "Distance-sensitive bloom filters," in Proc. of the Workshop on Algorithm Engineering and Experiments, 2006.

[9] S. Sultana, E. Bertino, and M. Shehab, "A provenance based mechanism to identify malicious packet dropping adversaries in sensor networks," in Proc. of ICDCS Workshops, 2011, pp. 332–338.

[10] 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.