Novelty Journals

ISSN 2394-7314

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (219-225), Month: January-April 2016, Available at: www.noveltyjournals.com

Enabling in Packet Bloom Filter Implementation for Adversary Wireless Sensor Network Environment

Amrutha Vardhini K S[1], Sumanth V[2]

2nd Year M.Tech, [2]Assistant Professor, Dept of CSE, RRIT, Bangalore

Abstract: **The numerous applications should work in Large-scale sensor networks domains. The data collected from wireless sensor network are used in making commitment in critical infrastructures. Data's are originated from multiple sources and transmitted through intermediate processing nodes. Those nodes perform the gathering of information. An attacker makes an agreement with those type of networks by introducing additional nodes in the network or compromising the existing nodes. So achieving the high data trustworthiness is crucial for correct decision-making. While evaluating the trustworthiness of sensor data provenance is an important factor. The several challenging requirements for provenance management in sensor networks are low energy and low bandwidth consumption, competent storage and secure transmission. This survey proposes a new lightweight scheme in order to securely transmit provenance with sensor data. The proposed in-packet Bloom filters techniques used to encode provenance with the sensor data. This mechanism initially performs provenance at the base station then perform reconstruction of the data at the base station. In addition to this the provenance scheme functionality used to detect packet drop attacks organized by malicious data forwarding nodes. This survey describes the effectiveness and efficiency of the Light weight secure provenance scheme in detecting packet forgery and packet loss attacks.**

Keywords: **Provenance; security; sensor networks; Packet drop attack; Wireless Sensor Networks; Provenance attack**.

I. INTRODUCTION

1.1 Data provenance at sensor network:

Sensor networks are used in various areas like such as cyber physical infrastructure systems, environmental weather monitoring, power grids, etc. Data are originated from a huge number of sensor node sources and they are processed at intermediate hops at in networks. These data's finally going to a base station (BS) which performs decision-making about where to go next. The uniformity of data sources creates assurance of the trustworthiness of data. This type of trustworthy information is considered in the decision making process at the base station. The data trustworthiness is assured by data provenance scheme. This is an effective method since it summarizes the history of ownership on the data and the list of actions performed on that information. The big advantage of this provenance scheme is detecting packet loss attacks organized by malicious/compromised sensor nodes. The major disadvantage of this scheme is the use of untrustworthy data at the nodes may create the catastrophic failures (e.g., SCADA systems). Although provenance modeling, collection, and querying have been used extensively in workflows [1] and curated databases [2], provenance at sensor networks has not been fully addressed.

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (219-225), Month: January-April 2016, Available at: www.noveltyjournals.com

1.2 In packet Boom Filter (iBF):

This is a distributed mechanism in order to encode provenance at the nodes and it will work as centralized algorithm to decode it at the BS. The technical core of this survey is the notion of (iBF) [3]. In this packet consists of a unique sequence number, data value, and an iBF which contains the provenance. The focus of this scheme is a securely transmitting provenance with the data to the BS. In this aggregation framework, securing the data values is an important factor,. The secure provenance technique can be used to obtain a complete solution that provides security for data, provenance and data-provenance binding.

The three Security Objectives in sensor networks is a confidentiality, Integrity and freshness.

1.2.1. Confidentiality:

An attacker by analyzing the contents of a packet cannot gain any knowledge about data provenance. Only authorized users (e.g., the BS) can process the information and check the integrity of provenance.

1.2.2. Integrity:

An attacker, acting individually or combining with others in a group, cannot add or remove non-colluding nodes. Also the attacker cannot add any data from the malicious user to the orginal data.

1.3.3. Freshness:

An attacker cannot replay the captured data from the original user and ensure the provenance detected by the BS. It is also important to provide a coupling between data and provenance i.e. Data-Provenance Binding, so the attacker cannot successfully drop or alter the legitimate/valid data while containing the provenance with the data, or swapping the provenance of two packets

1.3 Detecting Packet Drop Attacks:

Provenance encoding could be used for a packet acknowledgement. By using this sensor can transmit more meta-data. For an any individual 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 the intermediate packet could be drop by the attacker means some nodes on the path do not receive that packet. Hence, during the next round of packet transmission the mismatch between the acknowledgements should be generated from different nodes on the path. This factor could be to detect the packet drop attack and to localize the malicious node.

II. EXISTING SYSTEM

[2]In 2006 K. Muniswamy-Reddy et al, propose "Provenance- Aware Storage systems," .This survey states that in a multi-hop sensor network by using the data provenance scheme the BS can trace the source and forwarding path of an individual data packet. For each packet Provenance must be recorded but there is an important challenge arises due to the heavy storage, energy and bandwidth conditions of sensor nodes. So, it is necessary to provide a light-weight provenance socheme with low overhead.

Disadvantage:

- Sensors often operate in a un trusted environment, so there may chance of attacks.
- The necessary to address security requirements such as confidentiality, integrity and freshness of provenance should be increased.

[4]In 2005 R. Hasan et al proposes "threat model for wireless sensor networks". The assumption about the BS is it should be a trusted one, but if any other arbitrary node may be attacked means the also be changed to malicious. An attacker can eavesdrop and perform traffic analysis anywhere on the path. In addition to this he/she is able to organize a few malicious nodes, as well as compromise/attack a few legitimate nodes by capturing them and physically overwriting their memory. If an attacker compromises a node means it can extract all key materials, data, and codes stored on that node. The adversary can drop, inject or alter packets on the links which are under the control of attacker. Also the attacker can create

the denial of service attacks such as the complete removal of provenance. If a data packet does not contain no provenance records means it considered as highly suspicious data and hence generate an alarm/signal at the BS about this malicious packet arrival. To overcome this type of detection the attacker attempts to misrepresent the data provenance

[5] In 2012 S. Roy et al propose "Secure Data Aggregation in Wireless Sensor Networks," .This work deals with attacks against the synopsis diffusion. This aggregation work presents a lightweight verification algorithm to make verification at the BS. The several synopses generated should be verified independently by the verification protocol at three phases. The phases are query dissemination phase, aggregation phase and the verification phase. In the first phase called query dissemination phase, the BS broadcasts the aggregation name to compute a random seed. In second phase called the aggregation phase, each node computes a sub aggregate value based on the local value and the synopses of its children. The node also randomly selects a set of MACs .From the selected MACs check whether it should be the received ones from its children. Finally, in the third phase called verification phase, the BS computes the final synopses using the messages from its child nodes and verifies the received MACs.

Disadvantage:

- Employs separate transmission channels for data and provenance [6] but the provenance only requires a single channel for both.
- Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures [4], and they employ append-based data structures to store provenance, leading to prohibitive cost and time.

[7] In 2008 A. Ramachandran et al proposed "Packets with Provenance" .This scheme catches provenance for network packets in form of per packet tags. The captured information stores a history of all nodes and processes that packet and manipulates those packets. However, this scheme assures a trusted environment which is not practical in sensor networks.

[8]In 2010 W. Zhou et.al proposes "Querying and Maintenance of Network Provenance at Internet- Scale" which describes the history and sub part of the network state. This result came from the execution of a distributed protocol. The disadvantage of this system is also does not address security concerns and is specific to some network use cases.

[9] In 2011W. Zhou, et.al, proposes a "Secure Network Provenance," .This extends network provenance up to the adversarial environments. Even though all of these systems are general purpose network provenance systems but they are not optimized for the resource constrained sensor networks.

[10] In 2010 A. Syalim et al propose a "Preserving Integrity and Confidentiality of a Directed Acyclic Graph Model of Provenance," .The chain model of provenance ensure integrity(no one can change the data other than the original user) and confidentiality(no one can see the data other than original user)through encryption, checksum and incremental chained signature mechanism. Syalim et al. extend this method by applying digital signatures. This signature applied to a DAG model of provenance.

Disadvantage:

- These generic solutions are not aware of the sensor network specific assumptions, constraints, etc.
- Since provenance tends to grow very fast, transmission of a large amount of provenance information along with data will incur significant bandwidth overhead, hence low efficiency and scalability.

[11] In 2006 N. Vijaya kumar et al proposes "Towards Low Overhead Provenance Tracking in Near Real-Time Stream Filtering,". This system is an application specific system for near-real time provenance collection in data streams. Nevertheless, this system traces the source of a stream long after the process has completed.

[12] In 2010 Chong et al proposes" Self-Identifying Sensor Data". This scheme embeds the provenance of data source within the data. While it reflects the issues related to the confidentiality, Integrity and efficiency but it is not considered as a security mechanism. Also it does not deal with malicious attacks. However practical issues like scalability, data degradation have not been well addressed. In networking applications Bloom Filters are commonly used. In Packet Bloom Filters have only recently gained more attention being utilized in applications such as credential based data path security

[13], IP trace back [14], source routing and multicast [15], [16], etc. The basic idea in these works is to encode the link identifiers constituent to the packet routing path into an In Packet Bloom Filter.

Disadvantage:

- The encryption of the whole path is performed by the data source and the intermediate routers check their membership in the In Packet Bloom Filter and forward the packet further based on the decision. This approach is infeasible for sensor networks where the paths may change due to dynamic nature.
- An intermediate router only checks its own membership which may create several integrity attacks such as all-one attack, random bit flips, etc.

III. PROPOSED SYSTEM

The goal is to design a provenance encoding and decoding mechanism which satisfies security and performance needs. It proposes a provenance encoding strategy in that each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) should be transmitted along with the data. While receiving the packet the Base Station extracts and verifies the provenance information. The extension of the provenance encoding scheme allows the BS to detect packet drop attack organized by a malicious node. The features are

Formulate the problem of secure provenance transmission in sensor networks, and identify the challenges specific to this context.

Design an effective technique for provenance decoding and verification at the base station.

- Extend the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.
- Perform a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.

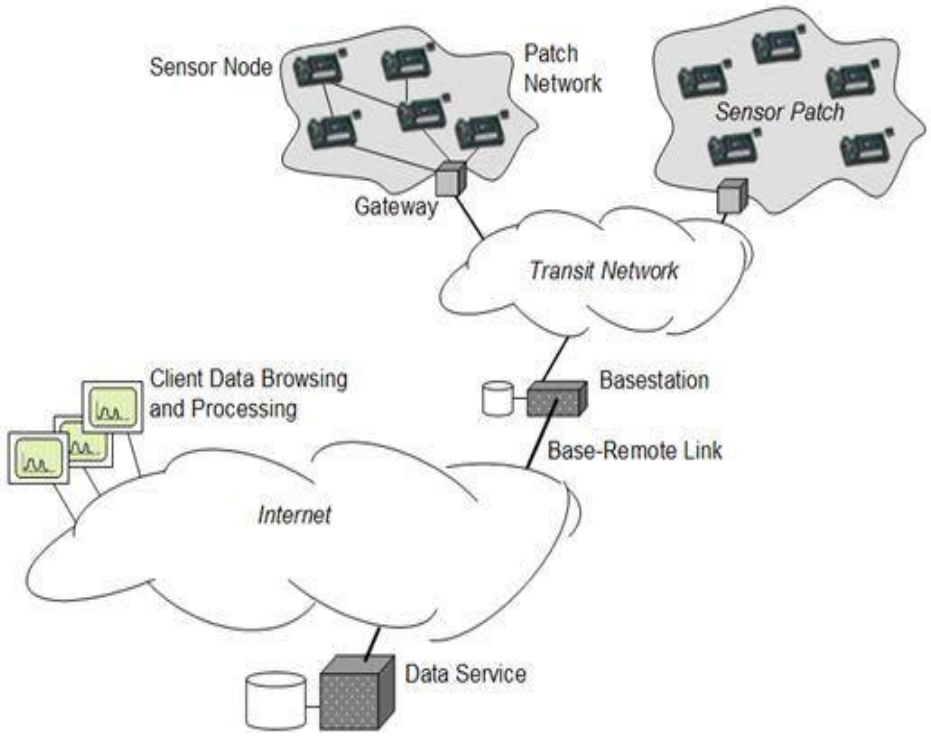

Fig 1. Architecture of Proposed system

International Journal of Novel Research in Computer Science and Software Engineering
Vol. 3, Issue 1, pp: (219-225), Month: January-April 2016, Available at: www.noveltyjournals.com

3.1 Advantages of Proposed System:

The fast message authentication code (MAC) schemes and Bloom filters are fixed-size data structures that efficiently represent provenance.

- Bloom filters make efficient usage of bandwidth, and they yield low error rates
- Claim for Confidentiality: - iBF is computationally infeasible to an attacker to gain data about the sensor nodes included in the provenance.
- Claim For Integrity: - An attacker, acting as single user or colluding with others in the group cannot successfully add or legitimate nodes to the data generated by the compromised/already attack happened nodes.
- An attacker or a set of cooperative attackers cannot selectively add or remove nodes from the provenance of data generated by legitimate nodes.
- A malicious aggregator cannot selectively drop a child node from the provenance.
- Claim For Freshness:- Provenance replay attacks are detected by the provenance scheme

Modules:

- Base station Module
- Network Formation Module
- Sender Module
- Intermediate Node Module
- Attacker Module

IV. METHODOLOGY

a. Base station

Base station will distribute the Encryption key to all nodes in the network. Then all nodes will receive the key and keep it. After the data is received from node, it will be performing Attack Analyzing task. It is used to check whether the data is affected in packet drop attack or forgery attack. If total number of packets is not matching with received packets then packet drop attack will be happened. If generated ibf and received ibf is not matching then it is affected by Forgery attack.

b. Network Formation:

Creating the Nodes and giving the path between those nodes. Every node should consist of Node id, Group id, IP address, sending port, receiving port. Shortest path finding is the process of listing all paths with corresponding energy. Assume there are 6 nodes in the network then, from source node to destination which is shortest path we going to identify using this module.

c. Sender Module:

Sender can select the text file to transfer to other node. The initial bloom filter (ibf) packet is always 0~0~0~0~0~0~0~0~0~0~0. Generate the sequence number for the path which is selected. Find the next hop node by adding plus one from current node. The pass the file content and one AES key and three hash code, sequence number and next node id. Encrypt the sequence number using key. Then get cipher text. Perform the hash code task and replace the ibf data with '1'. Then you will get new ibf. File will be converted as number of packets. We are setting packet size if 16 byte. If file content is not divisible by 16 then we are padding some characters at end of content. Next we splitting to 16 bytes of packets. Then data pattern is file_id##packet_id-current_packet (which is transferring currently)##sequence number##cipher text of packet##new_ibf; Then it will be transferred to next hop node.

d. Intermediate Node Module

Intermediate nodes will receive the data. It will be split and store in array. Here the sequence number will be encrypted with the help of intermediate node key. Then performed the same ibf task which we done in source module. If the attacker

node is attacking the current node then, it based on the random number value only packet drop or forgery node or both attacks need to perform attacks. Then the sequence number will be encrypted using the AES key. After that that ibf content will be replace with the help of hash code received. Atlast it will transfer to next hop node. Finally base station will receive the data.

e. Attacker Module:

Attacker module randomly select any node and attack the node and change the sequence number of that node

V. CONCLUSION

This survey addressed the problem of how securely transmitting provenance for sensor networks. Based on Bloom filters this paper proposed a light-weight provenance encoding and decoding scheme. The scheme ensures confidentiality, integrity and freshness of provenance. Also this scheme extended to incorporate data-provenance joining, and to include packet sequence information that supports detection of packet loss attacks. The proposed scheme is considered as effective, light-weight and scalable. This survey plan implements a real system prototype of secure provenance scheme, and to increase the accuracy of packet loss detection, especially in the case of multiple uninterrupted malicious sensor nodes.

ACKNOWLEDGMENT

We would like to thank Management of RRIT for providing such a healthy environment for the successful completion of this work and express my gratitude to Mr. Sumanth V. (Assistant Professor, RRIT, Bangalore) for providing continuous support and encouragement. Last but not the least I thank all my friends who has continuous support in all my works.

REFERENCES

[1] 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.

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

[3] 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.

[4] 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.

[5] 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.

[6] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Provenance in E-Science," ACMSIGMODRecord, vol. 34, pp. 31- 36, 2005.

[7] A. Ramachandran, K. Bhandankar, M. Tariq, and N. Feamster, "Packets with Provenance," Technical Report GT-CS-08-02, Georgia Tech, 2008.

[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 SIGMOD Int'l Conf. Management of Data, pp. 615-626, 2010.

[9] W. Zhou, Q. Fei, A. Narayan, A. Haeberlen, B. Loo, and M. Sherr, "Secure Network Provenance," Proc. ACMSOSP, pp. 295-310, 2011.

[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] 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.

[12] S. Chong, C. Skalka, and J.A. Vaughan, "Self-Identifying Sensor Data," Proc. Ninth ACM/IEEE Int'l Conf. Information Processing in Sensor Networks (IPSN), pp. 82-93, 2010.

[13] 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.

[14] R. Laufer, P. Velloso, D. Cunha, I. Moraes, M. Bicudo, M. Moreira, and O.Duarte, "Towards Stateless Single-Packet IP Traceback," Proc. 32nd IEEE Conf. LocalComputer Networks (LCN), pp. 548- 555, 2007.

[15] P. Jokela, A. Zahemszky, C. Esteve, S. Arianfar, and P. Nikander, "LIPSIN: Line Speed Publish/Subscribe Inter-Networking," Proc. ACM SIGCOMM Conf. Data Comm., pp. 195-206, 2009.

[16] A. Ghani and P. Nikander, "Secure In-Packet Bloom Filter Forwarding on the Netfpga," Proc. European NetFPGA Developers Workshop, 2010.