Volume 2, Issue 12, December 2016 ISSN NO: 2454 - 7514

North Asian International Research Journal Consortium

North Asian International Research Journal

Of

Science, Engineering and Information Technology

IRJIF IMPACT FACTOR: 3.821

NAIRJC JOURNAL PUBLICATION

North Asian International Research Journal Consortium

Welcome to NAIRJC

ISSN NO: 2454 -7514

North Asian International Research Journal of Science, Engineering & Information Technology is a research journal, published monthly in English, Hindi. All research papers submitted to the journal will be double-blind peer reviewed referred by members of the editorial board. Readers will include investigator in Universities, Research Institutes Government and Industry with research interest in the general subjects

Editorial Board

Address: -North Asian International Research Journal Consortium (NAIRJC) 221 Gangoo, Pulwama, Jammu and Kashmir, India - 192301, Cell: 09086405302, 09906662570, Ph. No: 01933-212815, Email: nairjc5@gmail.com, nairjc@nairjc.com, info@nairjc.com Website: www.nairjc.com

IRJIF IMPACT FACTOR: 3.821

IN-PACKET BLOOM FILTER: A PROVENANCE-BASED TRUSTWORTHINESS ASSESSMENT IN AD-HOC NETWORKS

MAYUR BAGUL [1], MILIND BHAGUNDE [2], DEEPALI BAWASKAR [3] & RASIKA GAWALI [4]

[1234] Department of Computer Engineering, Pune University, Pune India.

ABSTRACT

Now a day's networking become widely used thing in the world of computer science. Where popularity of sensor networks and their many uses in critical domains such as military and healthcare make them more vulnerable to malicious attacks. In such context, trustworthiness of senor data and their provenance is critical for decision making. Lots of time a malicious node or adversary may present an extra node in network like sensor network or ad-hoc network or it may compromise existing ones. In this paper we are representing an efficient and secure approach uses for transmitting provenance information about sensor data. Whatever we have developed uses super filters that are encoded as sensor data goes through various intermediate sensor nodes and they get decoded and verified at the base station. With the help of this developed technique our provenance technique will bale to defend against various malicious attacks done by unknown person or node. Such as packet drop and provenance forgery.

Keywords — Bloom filters, Provenance, Ad-hoc Networks, Security.

1. INTRODUCTION

Networking is become the most popular thing in the world of computer science. Along with networking, concept of internet is become one of the essential thing in our life. Hence in networking networks like sensor network, ad-hoc network and so many others kind of network lots of clients and user works as a part of network to which we generally called node. In this paper we will take example of sensor network which is used in lots of different application domain like military, hospitals, vehicular sensor network and so on. In a sensor network lots of data is get generated with the help of different nodes resides within network data of from large no. of source nodes is get processed in a network at intermediate hops towards their destination node. In this network trustworthiness of data is very important. We should be aware of of our transmitted data is reached safely to a destination node without any interfenace of another node. Hence diversity of data sources creates the need to assure the trustworthiness of data. For that purpose we are using the standard data provenance to know the trustworthiness

of data, it helps to get abstract view of history of ownership and the action performed on data. Here we have try to analyze the issues of secure and efficient provenance data transmission and processing of data. Also with that we are using the provenance of data for detecting the packet loss attack done by unknown node.

2. RELATED WORK

In a sensor network with the help of data provenance we can trace the source and forwarding path of an each and every data packet. Provenance for each data packet should be get store but apart from this challenges get arise due to energy, storage and bandwidth of sensor nodes. Therefore to give the solutions on these challenges it is essential to provide provenance solution with low overhead. As we know it can be happen that sensor nodes may work in non-trusted environment where they may get attacked by unknown malicious node. Hence it is very important to provide security constraints like confidentiality, accuracy and integrity of provenance. We are mainly focusing on to design the mechanism of provenance encoding and decoding that can fulfill the need of security and performance. With the help of pedigree it becomes possible to captures provenance in a network in the form of packet tags. Where nodes and processes manipulated the packets. However the exiting scheme considers an environment which is not realistic. In this paper we are proposing a model of provenance and ensure integrity and confidentiality through the encryption. Since the provenance tends to grow very fast, transmission of large amount of data provenance information along with data will incur significant bandwidth overhead, hence its results in low efficiency and scalability. Hence solution to this problem we propose a real time provenance collection in data stream.

- **Data Provenance**

After the analysis of existing research that mainly work with separate transmissions channel for provenance and data. But here in our paper we will be able to work with only single channel for both. Here in this paper we are implementing the provenance encoding at the base station. When user nodes or sensor node transmit data over a sensor network at that we assume node-level provenance in which node-level provenance encodes the sensor node at each steps of processing of the data. Like how we apply the methods for managing the trust of data and for detecting the attacks done by malicious node. We will consider d as data packet and provenance as directed acyclic graph G (V, E) .in this acyclic graph v (-V. which get directed to particular node HOST (v) =b which shows the provenance history. generally vertex in a provenance acyclic graph is identified by a vertex ID (VID) which is generated by sensor node using special functions like cryptography hash function. Main work of VID is

that it generates pre-packet based on given sequence numbers to and the secret key allocated by super filter algorithm. Once it get sequenced and attached with secret key it gets transmitted towards destination node.

- **Provenance Decoding:**

Here when the destination node gets the data from sender node it implements the standard provenance verification process. Which shows that the destination node have knowledge about data path and it checks the super filter to see whether the given data path is followed. Sometime it may happen that the data path through which data is get sent by source node may not be known to destination node in that case we need to apply provenance history collection process. Which consist and if needed it retrieves the provenance from a source node.

3. SYSTEM ARCHITECTURE

System architecture consists of following components:-

1. Sender node
2. Intermediate node/Malicious node
3. Malicious node

1) Sender node :-

We send our data from sender node. Before sending data is encrypted with public key. In this our data is first divide into number of packets then we assign sequence number to each packet.

2) Intermediate node/Malicious node:-

This node may be intermediate node or malicious node. When data is transmitted from sender node to intermediate node. It may be attacked in between by some malicious node. Malicious node can change the base station address. This node may drop some packets in the sender node also they can forged some data in it. Here we used IP tracing scheme. IP tracing detects that data come from which IP address also to which IP address it has to be transmitted. Then by tracing IP data, intermediate node sends data to actual base station.

3) Receiver node :-

When the receiver receives a data packet, it executes the provenance verification process, which assumes that the base station knows what the data path should be, and checks the In-Packet Bloom Filter algorithm to see whether the correct path has been followed. Provenance decoding is done at receiver side. Provenance data is decoded and verified at base station only.

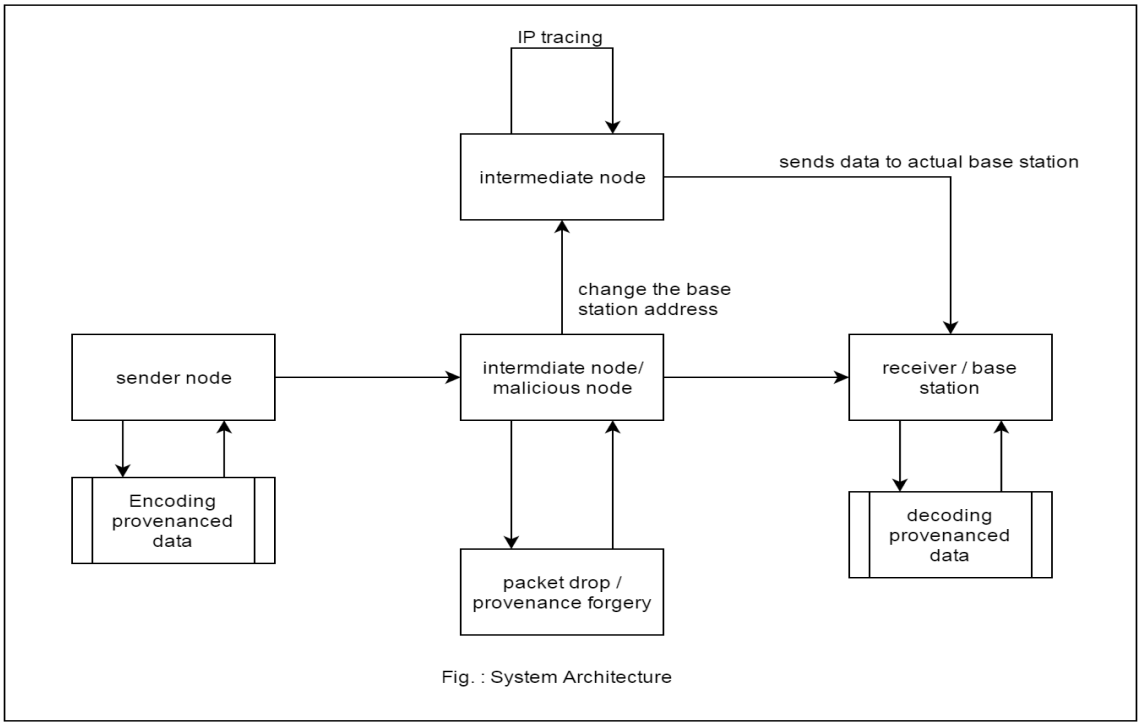

Fig. : System architecture of proposed System.

4. PURPOSE AND SCOPE

Project scope contains developing the new bloom filters which securely transmit the sensor data more efficiently than previously used bloom filters. Here we use three different algorithms i.e. In-Packet Bloom filter algorithm, provenance encoding and decoding algorithm.

Sensor networks are becoming so popular in numerous application domains such as power grids, environmental monitoring etc. Data provenance is an effective method to assess data trustworthiness, since it summarizes the history of ownership and the actions performed on the data. 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.

APPLICATIONS

1) Military Application
2) Healthcare System.
3) VANET etc.

5. CONCLUSION

In this paper we have used light-weight In-Packet Bloom filters that are encoded as sensor data travels through intermediate sensor nodes, and are decoded and verified at the base station. Our provenance technique is also able to defend against malicious attacks such as packet dropping and allows one to detect the responsible node for packet drops.

6. ACKNOWLEDGEMENT

We are thankful to our project guide Prof. Ashwini Jadhav for their support. Also all the staff of Computer Department for coordination.

7. REFERENCES

[1] S.Sultana, G.Ghinita, E.Bertino, and M. Shehab , "A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks," IEEE Transactions on Dependable and Secure Computing vol.6 , no.1, January 2016. (done)

[2] 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.

[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] 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.

[5] P. Jokela, A. Zahemszky, C.E.Rothenberg, S. Arianfar, and P. Nikander, "LIPSIN: Line Speed Publish/Subscribe Inter-Networking" .

[6] A. Kirsch and M. Mitzenmacher, "Distance-sensitive bloom filters," in *Proc. of the Workshop on Algorithm Engineering and Experiments*, 2006, pp. 41–50.

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An efficient clustering based heuristic for data gathering and aggregation in sensor networks," in *Proc. of Wireless Communications and Networking Conference*, 2003, pp. 1948–1953.

[8] 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.

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

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

Publish Research Article

Dear Sir/Mam,

We invite unpublished Research Paper,Summary of Research Project,Theses,Books and Book Review for publication.

Address:- North Asian International Research Journal Consortium (NAIRJC)
221, Gangoo Pulwama - 192301
Jammu & Kashmir, India
Cell: 09086405302, 09906662570,
Ph No: 01933212815
Email:- nairjc5@gmail.com, nairjc@nairjc.com , info@nairjc.com
Website: www.nairjc.com