# Secured Provenance System for Data Transmission in Wireless Sensor Networks

P.MAITREYI
Assistant Professor, Research Scholar
Dept. of IT, M.G.I.T,
T.S., INDIA

Dr. M. SREENIVAS RAO
Professor of Computer Science
JNTUH, T.S, India
T.S, INDIA

## INTRODUCTION

Sensor networks are acclimated in abundant appliance domains, such as cyber concrete basement systems, ecology monitoring, ability grids, etc. Abstracts are produced at a ample amount of sensor bulge sources and candy in-network at average hops on their way to a Abject Abject (BS) that performs decision-making. The assortment of abstracts sources creates the charge to assure the abidingness of data, such that alone accurate advice is advised in the accommodation process. Abstracts ancestry is an able adjustment to appraise abstracts trustworthiness, back it summarizes the history of buying and the accomplishments performed on the data. Recent assay accent the key addition of ancestry in systems breadth the use of capricious abstracts may advance to adverse failures (e.g., SCADA systems). Although ancestry modeling, collection, and querying accept been advised abundantly for workflows and curated databases, ancestry in sensor networks has not been appropriately addressed. We investigate the botheration of defended and able ancestry manual and processing for sensor networks, and we use ancestry to ascertain packet accident attacks staged by awful sensor nodes. In a multi-hop sensor network, abstracts ancestry allows the BS to trace the antecedent and forwarding aisle of an alone abstracts packet. Ancestry accept to be recorded for anniversary packet, but important challenges appear due to the bound storage, activity and bandwidth constraints of sensor nodes. Therefore, it is all-important to devise a light-weight ancestry band-aid with low overhead. Furthermore, sensors generally accomplish in an untrusted environment, breadth they may be accountable to attacks. Hence, it is all-important to abode aegis requirements such as confidentiality, candor and blossom of provenance. Our ambition is to architecture a ancestry encoding and adaptation apparatus that satisfies such aegis and performance needs. We adduce a ancestry encoding action whereby anniversary bulge on the aisle of a abstracts packet deeply embeds ancestry advice aural a Blossom clarify that is transmitted forth with the data. Upon accepting the packet, the BS extracts and verifies the ancestry information. We aswell devise an addendum of the ancestry encoding arrangement that allows the BS to ascertain if a packet bead advance was staged by a awful node. As against to absolute assay that employs abstracted manual channels for abstracts and provenance, we alone crave a individual approach for both. Furthermore, acceptable ancestry aegis solutions use assiduously cryptography and agenda signatures, and they apply append-based abstracts structures to abundance provenance, arch to prohibitive costs. In contrast, we use alone fast Bulletin Affidavit Cipher (MAC) schemes and Blossom filters (BF), which are fixed-size abstracts structures that compactly represent provenance. Blossom filters accomplish able

acceptance of bandwidth, and they crop low absurdity ante in practice. Our specific contributions are as follows.

• We codify the botheration of defended ancestry manual in sensor networks, and analyze the challenges specific to this context;

• We adduce an in-packet Blossom clarify ancestry encoding scheme

• We architecture able techniques for ancestry adaptation and assay at the abject station.

• We extend the defended ancestry encoding arrangement and devise a apparatus that detects packet bead attacks staged by awful forwarding sensor nodes.

• We accomplish a abundant aegis assay and achievement appraisal of the proposed ancestry encoding arrangement and packet accident apprehension mechanism.

## A BRIEF STUDY OF PREVIOUS SOLUTIONS AND OUR SOLUTION

In the alpha of this chapter, we try and accept the botheration we are about to accord with.

We are alive to architecture a band-aid that can accouterment the botheration of modification of abstracts and bead of packets of abstracts in a wireless sensor network. Several solutions accept been advised in this breadth and they are as follows.

### EXISTING SYSTEM

•Recent assay accent the key addition of ancestry in systems breadth the use of capricious abstracts may advance to adverse failures (e.g., SCADA systems). Although ancestry modeling, collection, and querying accept been advised abundantly for plan flows and curated databases, ancestry in sensor networks has not been appropriately addressed.

### DISADVANTAGES OF EXISTING SYSTEM

•Traditional ancestry aegis solutions use assiduously cryptography and agenda signatures, and they apply append-based abstracts structures to abundance provenance, arch to prohibitive costs.

•Existing assay employs abstracted manual channels for abstracts and provenance.

### PROPOSED SYSTEM

- We investigate the botheration of defended and able ancestry manual and processing for sensor networks, and we use ancestry to ascertain packet accident attacks staged by awful sensor nodes.

- Our ambition is to architecture a ancestry encoding and adaptation apparatus that satisfies such aegis and achievement needs. We adduce a ancestry encoding action whereby anniversary bulge on the aisle of a abstracts packet deeply embeds ancestry advice aural a Blossom clarify (BF) that is transmitted forth with the data. Upon accepting the packet, the BS extracts and verifies the ancestry information. We aswell devise an addendum of the

ancestry encoding arrangement that allows the BS to ascertain if a packet bead advance was staged by a awful node.

## ADVANTAGES OF PROPOSED SYSTEM

•We use alone fast bulletin affidavit cipher (MAC) schemes and Blossom filters, which are fixed-size abstracts structures that compactly represent provenance. Blossom filters accomplish able acceptance of bandwidth, and they crop low absurdity ante in practice.

•We codify the botheration of defended ancestry manual in sensor networks, and analyze the challenges specific to this context.

•We adduce an in-packet Blossom clarify (iBF) provenance-encoding scheme.

•We architecture able techniques for ancestry adaptation and assay at the abject station.

•We extend the defended ancestry encoding arrangement and devise a apparatus that detects packet bead attacks staged by awful forwarding sensor nodes.

•We accomplish a abundant aegis assay and achievement appraisal of the proposed ancestry encoding arrangement and packet accident apprehension mechanism.

•We alone crave a individual approach for both manual channels for abstracts and provenance.

It aswell specifies the accouterments and software requirements that are appropriate in adjustment to run the appliance properly. The Software Claim Specification (SRS) is explained in detail, which includes overview of this argument as able-bodied as the anatomic and non-functional claim of this dissertation.

## MODULES

### NODE CONFIGURATION

#### A.LINK CONFIGURATION

In this bore Nodes are configured based on amount of nodes in charge of packet requisition. We actualize the arrangement accumulation by abutting nodes to sink. Link agreement agency abutting the nodes and average nodes to the sink.

### SENDER NODE

#### A.PACKET SPLITTING

In this module, Sender selects the file which is to be sent. And then it split into the number of packets based on the size for adding some bits in it.

**B.SEND PACKETS TO INTERMEDIATE**

And then it encrypts all the splitted packets. And then sender adds some bits to each encrypted packets before sending that. Bit Addition for each packet is identification for sender. After adding of bits to each packet, it sends the packets to the nearest node or intermediate node.

**INTERMEDIATE NODE(ROUTER)**

**A.SEND PACKETS TO SINK**

In this module, the intermediate node receives Packets from the sender. After receiving all packets from sender, it encrypts all packets again for authentication. Before sending to sink, intermediate add some bits to each packet for node identification. After adding some bits from intermediate, it sends all packets to the sink.

**B.MODIFY OR DROP**

Before sending all packets to sink, packets bottomward or packets modifying may be action in intermediate.

**SINK**

**A.VERIFY**

In this module, Bore receives all packets from the sender node, and it verifies all packets which are alone or not. And it aswell verifies the packets which are adapted or not and it can analyze the modifiers in the action based on the bit identification.

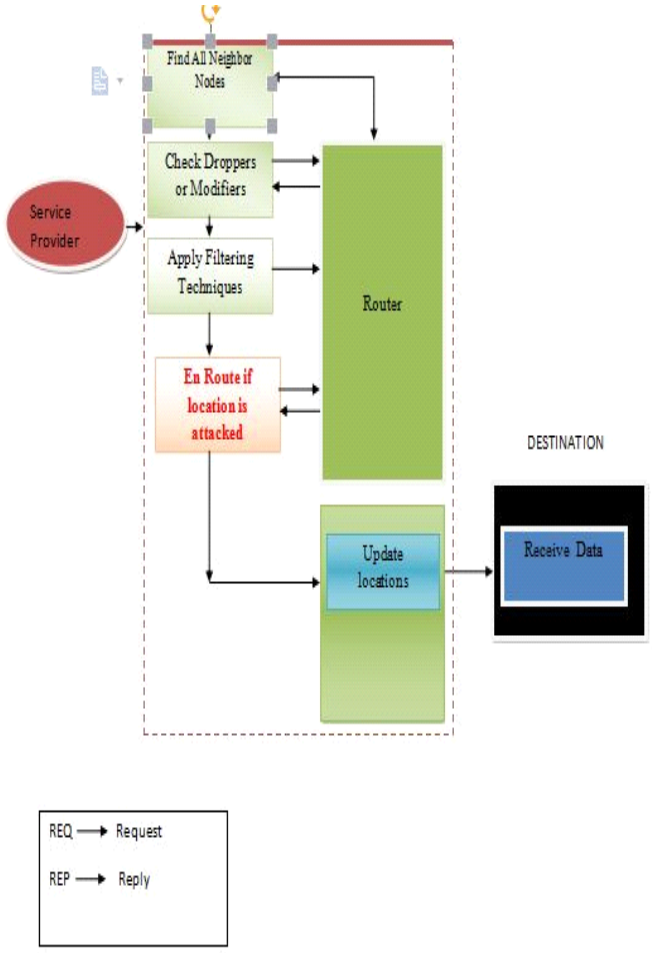
**B.MERGE PACKETS**

After accepting all packets in sink, it decrypts all packets. After the decryption if there is no adapted or alone packets, it absorb all packets. After merging, Bore can accept the aboriginal file.

**C.CATEGORIZATION AND RANKING**

In this bore Categorization and Baronial will be performed based on the bulge behavior. If there is any modification or bead of packets in bulge it assumes abrogating amount for modifier or dropper. Bore performs Baronial for anniversary bulge based on the Category of nodes. Bore gives baronial like Good, Temporarily Good, Suspiciously Bad, Bad based on the bulge behavior in the process

## SYSTEM ARCHITECTURE:




## CONCLUSION

We addressed the botheration of deeply transmitting ancestry for sensor networks, and proposed a light-weight ancestry encoding and adaptation arrangement based on Blossom filters. The arrangement ensures confidentiality, candor and blossom of provenance. We continued the arrangement to absorb data-provenance binding, and to cover packet arrangement advice that supports apprehension of packet accident attacks. Experimental and analytic appraisal after-effects appearance that the proposed arrangement is effective, light-weight and scalable. In approaching work, we plan to apparatus a absolute arrangement ancestor of our defended ancestry scheme, and to advance the accurateness of packet accident detection, abnormally in the case of assorted after awful sensor nodes.

## FUTURE ENHANCEMENTS/ RECOMENDATIONS

In the accepted adaptation of implementation, we accept not advised the case of after awful nodes. We plan to architecture a arrangement of accomplishing for the mentioned requirement. Approaching plan can aswell be agitated out to advance the accurateness of packet accident detection.

## REFERENCES

[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] 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. on 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 AnnualTechnical Conf.*, 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. Hellerstin, and W. Hong, "TAG: a tiny aggregation service for ad-hoc sensor networks," *SIGOPS Operating Systems Review*, no. SI, Dec. 2002.

[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] 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.

[9] L. Fan, P. Cao, J. Almeida, and A. Z. Broder, "Summary cache: a scalable wide-area web cache sharing protocol," *IEEE/ACM Trans. Netw.*, vol. 8, no. 3, pp. 281–293, Jun. 2000.

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

[11] C. Rothenberg, C. Macapuna, M. Magalhaes, F. V rdi, and A. Wiesmaier, "In-packet bloom filters: Design and networking applications," *Computer Networks*, vol. 55, no. 6, pp. 1364 – 1378, 2011.

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof sketches: Verifiable in-netwok aggregation," in *ICDE*, 2007, pp. 84–89.

[13] T. Wolf, "Data path credentials for high-performance capabilitiesbased networks." in *Proc. of ACM/IEEE Symp. on Architectures for Networking and Communications Systems.*, 2008, pp. 129–130.

[14] H. Chan, A. Perrig, and D. Song, "Secure hierarchical in-network aggregation in sensor networks," in *Proc. of the conf. on Computer and communications security (CCS)*, 2006, pp. 278–287.

[15] 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.

**Author Profile 1:**

Ponguwala Maitreyi is currently a researcher in JNUH. She received her M.Tech in Computer Science from JNTUH and B.Tech degree in Computer Science and Information Technology from JNTU Hyderabad. She has published research papers in reputed National & International Journals. She is Assistant Professor at Department of Information Technology, Mahathma Gandhi Institute of Technology, Hyderabad. Her areas of interest are Adhoc and Sensor Networks, Wireless Networks and Mobile Communications, Network security and Cryptography and Network Programming

**Author Profile 2:**

Dr. M. Sreenivasa Rao, is the current Director Academic Audit Cell, JNTUH and also Professor of SIT Computer Science. He performs both his roles with ease. He is indeed a widely read and active person in the academic front. His articles and publications are published all over the world.