ISSN 2394-3777 (Print)
ISSN 2394-3785 (Online)
Available online at www.ijartet.com
International Journal of Advanced Research Trends in Engineering and Technology (IJARTET)
Vol. 3, Special Issue 15, March 2016

Secure Transmission Against Provenance Forgery And Packet Drop Attacks In Wireless Sensor Networks

A.Rachel Roselin[1],
M.E., Computer Science Student,
M.I.E.T Engineering College, Trichy,
roseruby1993@gmail.com

G.Nalina Keerthana[2]
Assistant Professor, Department of CSE,
M.I.E.T Engineering College, Trichy
jjkgnk@gmail.com

R.Bhuvaneshwari[3]
M.E., Computer Science Student,
M.I.E.T Engineering College, Trichy
bhuvanarkcse@gmail.com

***Abstract*—**. Data are flowed from various sources through transitional processing nodes that aggregate information and cruel opposition may introduce extra nodes in the network or compromise existing ones, assuring high data trustworthiness is crucial for correct decision-making. Data provenance (origin) represents a key factor in evaluating the trustworthiness of sensor data. A lightweight scheme has been proposed, to securely transmit provenance for sensor data, that technique relies on in-packet Bloom filters to encode provenance. An competent mechanism has been introduced for provenance verification and reform at the base station. The secure provenance scheme can be extended with functionality to detect packet drop attacks dramatic by cruel data forwarding nodes. The proposed technique has been evaluated to prove the effectiveness and efficiency of the trivial secure provenance scheme in detecting packet forgery and loss attacks in wireless network environments.

***Key words*—Provenance,Security,Bloom Filter,Packet Drop.**

I. INTRODUCTION

Sensor networks are used in application domains such as cyber physical communications, ecological checking, whether monitoring power grids, etc. The data that should be large sensor node sources and processed in-network with their way to a Base Station (BS) that performs which decision should be taking. Information is considered in the decision process or making. Data provenance is an effective method to assess data trustworthiness, and the actions performed on the data. Provenance in sensor networks has not been present properly addressed. Investigate the problem of secure and efficient provenance transmission and handling for sensor networks, and we use origin to detect packet failure attacks dramatic by cruel sensor nodes. In a multi-hop sensor network, data origin allows the BS to trace the source and forwarding path of an individual data packet. Origin must be witnessed for each packet, but important tests arise due to the tight storage, energy and bandwidth of sensor nodes. More sensors often operate in an untrusted environment, it may be subject to show aggressions. To address the security such as confidentiality, integrity and freshness of provenance. Propose a provenance encoding strategy for each node on the data packet securely embeds provenance data with a Bloom filter (BF) that is transmitted along with the data. Upon on receiving the packet, the BS extracts and prove the provenance information. To extend the provenance encoding scheme allows the BS to detect packet drop attacks during the sensor node transmission. In the existing research that employs separate transmission channels for data provenance, it only requires a single channel for both. Usual origin security solutions use seriously cryptography and digital signatures and they employ appended based data structures to store provenance, leading to prohibit costs. Use message authentication code (MAC) schemes and Bloom filter, which are fixed-size data structures that compactly represent provenance.

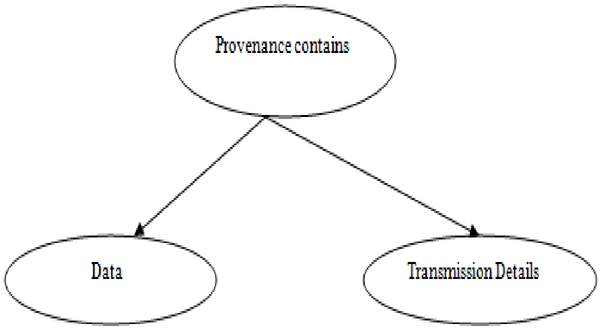

Fig. 1. Provenance

A. Related Works

Let us discuss some of the previous work done in this area. Provenance security, and time based flow watermarking. a lot of work regarding active-timing based watermarking for network flow, watermarking scheme extensively differs from these approaches in various aspects. (i) All of these schemes insert a single watermark message over the IPDs of a flow. On the contrary, to allow various nodes to watermark origin over the same set of IPDs. (ii) Our decoding process is completely different since it does not recover the embedded origin by gathering tad from each IPD. Instead, of use a single approach based on a cross-correlation and threshold based mechanism (iii) Several mechanisms watermark a bit by controlling the data throughput for a certain amount of time whereas to prolong the IPD by a small amount of time A chain model of provenance and guarantee consistency and confidentiality through encryption, checksum and incremental chained signature. Extends this method by applying digital signature to a DAG model of origin. However, these general solutions are not sensitive of the sensor network attributes. Since origin tends to grow very prompt, transmission of a large amount of origin information along with data earns large bandwidth overhead and looses efficiency and scalability. ExSPAN describes the record and sources of network state that result from the execution of a dispersed protocol. This system also does not address security concerns and is definite to some network use cases. SNP extends network provenance to adversarial environments. Embed the origin of data source inside the data set. While it reflects the importance of issues are addressed, it is not intended as a security mechanism, hence, does not deal with cruel attacks.

B. Contributions

Introduce an algorithm for provenance verification The Provenance verification is the first algorithm used for verify provenance. The BS conducts the verification process not only to verify its knowledge of provenance but also to check the integrity of the transmitted provenance. Imagine that the knowledge of the BS on this packet’s path is P0. At first, the BS initializes a Bloom filter BFc with all 0’s. The BF is then updated by generating the VID for each node in the path P0 and inserting this ID into the BF. BFc now reflects the perception of BS about the encoded provenance. To validate its view, the BS then compares BFc to the received iBF. The provenance verification succeeds only if BFc is equal to iBF. Otherwise, if BFc differs from the received iBF, it indicates either a change in the data flow path or a BF modification attack. The verification failure triggers the provenance collection process which attempts to retrieve the nodes from the encoded provenance and also to distinguish between the events of a path change and an attack. Christo Ananth et al. [5] discussed about a method, Wireless sensor networks utilize large numbers of wireless sensor nodes to collect information from their sensing terrain. Wireless sensor nodes are battery-powered devices. Energy saving is always crucial to the lifetime of a wireless sensor network. Recently, many algorithms are proposed to tackle the energy saving problem in wireless sensor networks. There are strong needs to develop wireless sensor networks algorithms with optimization priorities biased to aspects besides energy saving. In this project, a delay-aware data collection network structure for wireless sensor networks is proposed based on Multi hop Cluster Network. The objective of the proposed network structure is to determine delays in the data collection processes. The path with minimized delay through which the data can be transmitted from source to destination is also determined. AODV protocol is used to route the data packets from the source to destination.

To propose an in-packet Bloom filter (iBF) provenance-encoding scheme. Design efficient techniques for provenance decoding and verification at the base station and extend the secure provenance encoding scheme and plan a mechanism that detects packet crash attacks staged by malicious forwarding sensor nodes. To perform a complete security analysis and performance assessment of the planned provenance encoding scheme and packet failure finding mechanism.

II. SYSTEM MODEL

Systems design is just a design of systems. It implies a regular and exact approach to design an approach insisted by the scale and complexity of many systems problems. A systems approach to design is completely compatible with a user-centred approach. Certainly, the interior of both approaches understands user objects. A systems advance looks at users in relation to a framework and in terms of their communication with devices, with each other, and with themselves. A systems advance to design is most suitable for projects connecting large systems or systems of systems. Such projects typically involve many people, from many disciplines, working together over an comprehensive period of time. They need tools to cope with their project’s complexity: to define goals, assist communications, and manage processes. Singly designers working on small projects may find the same tools a bit cumbersome for their needs.

A. Data Stream Module

Sensor networks are used in numerous application domains, such as cyber physical infrastructure systems, ecological monitoring, power grids, etc. Data are produced at a large number of sensor node sources and processed in-network at middle hops on their way to a base station (BS) that performs decision making. Believe a multihop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network. The BS assigns each node a unique identifier nodeID and a symmetric cryptographic key Ki. In addition, a set of hash functions H={h1, h2, . . . , hk} are broadcast to the nodes for use during provenance embedding. Each sensor generates data regularly, and individual values are aggregated towards the BS using any existing hierarchical dissemination scheme. A data path of D hops is represented as <nl, n1, n2,. . . , nD >, where nl is a leaf node representing the data source, and node ni is i hops away from nl. Each non-leaf node in the path aggregates the received data and provenance with its own locally-generated data and provenance.

B. provenance Management Module

Given packet d, its provenance is modelled as a directed acyclic graph G(V,E) where each vertex(v U V) is attributed to a specific node HOST(v)= n and represents the origin record (nodeID) for that node. Each vertex in the provenance graph is uniquely recognized by a vertex ID (VID) which is generated by the host node using cryptographic hash functions. The edge set E consists of directed edges that connect sensor nodes. Data provenance is an effective method to assess data trustworthiness, since it summarizes the record of possession and the actions performed on the data. In a multi-hop sensor network, data provenance allows the BS to trace the source and forwarding path of an individual data packet. Provenance must be recorded for each packet, storage, energy and bandwidth constraints of sensor nodes. Therefore, it is necessary to devise a light-weight origin solution with low overhead. Furthermore, sensors often operate in an untrusted environment, where they may be focus to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance.

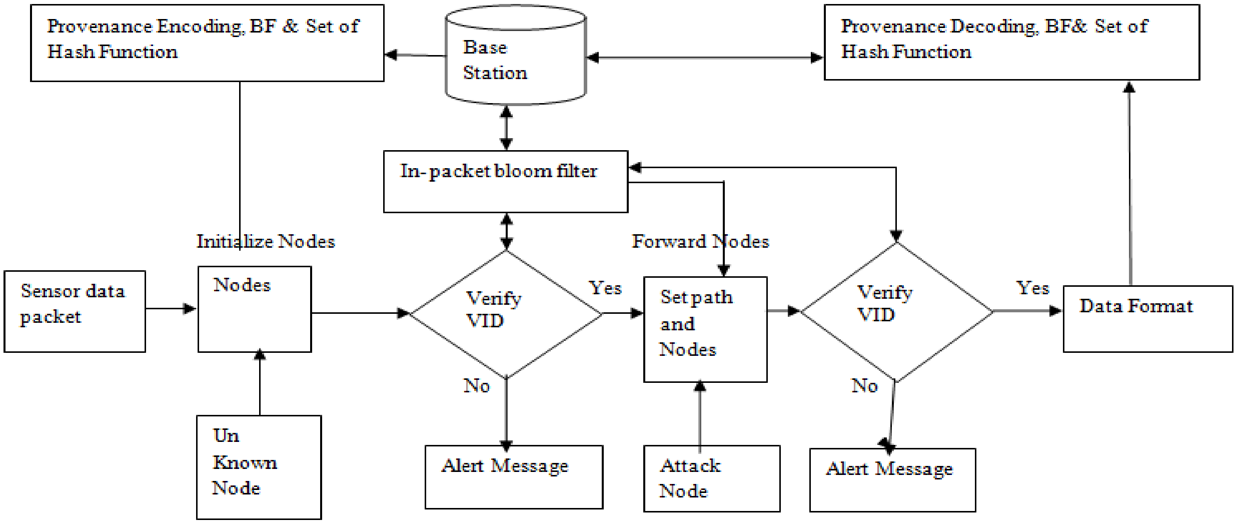

Fig. 2. System Architecture

C. Encode provenance Security

Each packet consists of a unique sequence number, data value, and an iBF which holds the provenance, focus is on securely transmitting provenance to the BS. In an aggregation infrastructure, securing the data values is also an important aspect, secure provenance technique can be used in conjunction with such work to obtain a entire solution that provides security for data, provenance and data-provenance binding. For a data packet, provenance encoding refers to generating the vertices in the provenance graph and inserting them into the iBF.

Each vertex creates at a node in the data path and represents the provenance record of the host node. A vertex is uniquely identified by the vertex ID. The VID is generated per-packet based on the packet sequence number (seq) and the secret key Ki of the host node. We use a block cipher function to produce this VID in a secure manner. A Provenance encoding scheme whereby each node on the path of a data packet securely embeds provenance information inside a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. Also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a cruel node. Not only the intermediate nodes, but also the BS stores and updates the latest packet sequence number for each data flow. Upon receiving a packet, the BS retrieves the preceding packet sequence (pSeq) transmitted by the source node from the packet header, fetches the last packet sequence for the flow from its local storage (pSeqb), and utilizes these two sequences in the process of provenance verification and collection.

D. Detect Attack Module

Differs from the received iBF, it indicates either a change in the data flow path or a BF modification attack. The verification failure triggers the provenance collection process which attempts to retrieve the nodes from the encoded provenance and also to distinguish between the events of a path change and an attack. Such an inference might introduce errors because of false positives If the verification succeeds, decide that there was a natural change in the data path and have been able to determine the path correctly.

Otherwise, an attack has occurred. If the data aggregation result is verified at the BS, then the data provenance coupling is ensured at each node in the routing path. Against attacks the précis diffusion and Lightweight verification algorithm to verify at BS if the computed overall is correct. This algorithm is user to sense packet drop from cruel nodes. The BS computes the final synopsis using the messages from its child nodes and verifies the received MACs.

III. PERFORMANCE EVALUATION

Implement In a multi-hop sensor network launches efficient mechanisms for provenance verification and reform at the base station. In addition, extend the secure provenance scheme with functionality to sense packet drop attacks staged by cruel data forwarding nodes. Evaluate the proposed technique results prove the effectiveness and efficiency of the lightweight secure origin scheme in sensing packet forgery and loss attacks.

IV. CONCLUSION

Addressed the problem of securely conveying origin for sensor networks, and proposed a light-weight provenance encoding and decoding system based on Bloom filters. The scheme ensures confidentiality, integrity and freshness of provenance, extended the scheme to incorporate data-provenance binding, and to include packet sequence information that supports finding of packet loss attacks. Experimental results show that the proposed scheme is effective, light-weight and scalable.

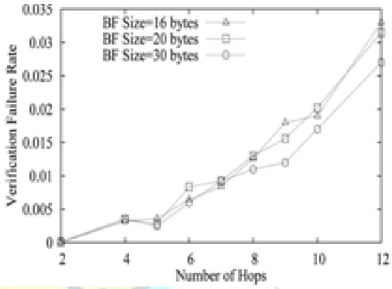

Fig. 3. Percentage of collection error

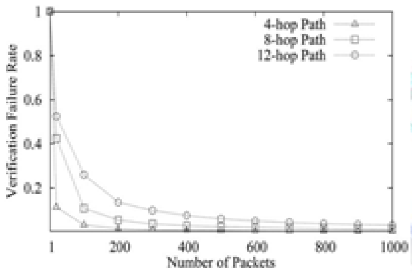

Fig. 4. False positive rate

V. FUTURE ENHANCEMENT

In future work, our secure provenance scheme, plan to implement a real system prototype of with temporary and alternative association malicious Nodes environments and improve the accuracy of packet loss detection, especially in the case of multiple consecutive malicious sensor nodes.

REFERENCES

[1] Ghani. A and Nikander. P. (2010), ‘Secure In-Packet Bloom Filter Forwarding on the Netfpga’, Proc. European NetFPGA Developers Workshop.

[2] R.Hasan , R.Sion, and M.Winslett. (2009), ‘The Case of the Fake Picasso: Preventing History Forgery with Secure Provenance’, Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14.

[3] H.Lim , Y.Moon , and Bertino E. (2010), ‘Provenance-Based Trustworthiness Assessment in Sensor Networks’, Proc. Seventh Int’l Workshop Data Management for Sensor Networks, pp. 2-7.

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

[5] Christo Ananth, T.Rashmi Anns, R.K.Shunmuga Priya, K.Mala, “Delay-Aware Data Collection Network Structure For WSN”, International Journal of Advanced Research in Biology, Ecology, Science and Technology (IJARBEST), Volume 1,Special Issue 2 - November 2015, pp.17-21

[6] Sultana S, Bertino E, and Shehab M. (2011) ’Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks’, Proc. Int’l Conf. Distributed Computing Systems (ICDCS) Workshops. pp. 332-338

[7] Sultana S, Shehab M, and Bertino E. (2013), “Secure Provenance Transmission for Streaming Data,” IEEE Transactions. Knowledge and Data Eng., vol. 25, no. 8, pp. 1890-1903.

[8] Zhou W, Fei Q, Narayan A, Haeberlen A, Loo B and Sherr M. (2011), “Secure Network Provenance,” Proc. ACMSOSP, pp. 295-310.

[9] Zhou W, Sherr M, Tao T, Li X, Loo B, and Mao Y. (2010), ‘Efficient Querying and Maintenance of Network Provenance at Internet-Scale’, Proc. ACM SIGMOD Int’l Conf. Management of Data, pp. 615-626.

[10] Madden S, Franklin J, Hellerstein J, and Hong W, “TAG: A Tiny Aggregation Service for Ad-Hoc Sensor Networks,” ACM SIGOPS Operating Systems Rev., vol. 36, no. SI, pp. 131-146, Dec. 2002.

[11] Dasgupta K, Kalpakis K, and Namjoshi P, “An Efficient Cluster- ing Based Heuristic for Data Gathering and Aggregation in Sensor Networks,” Proc. Wireless Comm. and Networking Conf., pp. 1948-1953, 2003.

[12] Sultana S, Bertino E, and Shehab M, “A Provenance Based Mechanism to Identify Malicious Packet Dropping Adversaries in Sensor Networks,” Proc. Int’l Conf. Distributed Computing Systems (ICDCS) Workshops, pp. 332-338, 2011.

[13] Fan L, Cao P, Almeida J, and Broder A.Z , “Summary Cache: A Scalable Wide-Area Web Cache Sharing Protocol,” IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

[14] Kirsch A and Mitzenmacher M, “Distance-Sensitive Bloom Filters,” Proc. Workshop Algorithm Eng. and Experiments, pp. 41-50, 2006.

[15] Wolf T, “Data Path Credentials for High-Performance Capabili- ties-Based Networks,” Proc. ACM/IEEE Symp. Architectures for Net- working and Comm. Systems, pp. 129-130, 2008.

AUTHORS

A.Rachel Roselin, She has received B.E Computer science and Engineering degree from Mount Zion college of engineering and technology, Pudukkottai in 2014 and currently pursing ME Computer science and Engineering degree in M.I.E.T engineering college, Trichy .

E-mail:roseruby1993@gmail.com

Mrs.G.Nalina Keerthana, She has received B.E Information Technology degree from J.J college of engineering and technology , Trichy in 2004 and ME Computer science and Engineering degree in M.I.E.T engineering college, Trichy in 2013

E-mail:roseruby1993@gmail.com

R.Bhuvaneshwari, She has received B.E Computer science and Engineering degree from Mount Zion college of engineering and technology, Pudukkottai in 2014 and currently pursing ME Computer science and Engineering degree in M.I.E.T engineering college, Trichy .

E-mail:bhuvanarkcse@gmail.com