International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

IJIEMR Transactions, online available on 5th Dec 2017. Link
:http://www.ijiemr.org/downloads.php?vol=Volume-6&issue=ISSUE-12

Title : SECURE SCHEME FOR DETECTING PROVENANCE FORGERY AND POCKET DROPS IN WIRELESS SENSOR NETWORKS

Volume 06, Issue 12, Pages: 97–104.
Paper Authors

C ARUN KUMAR, CS.MAHABOOBBEE, M VENKATESH NAIK
CRIT , Anantapur

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

SECURE SCHEME FOR DETECTING PROVENANCE FORGERY AND POCKET DROPS IN WIRELESS SENSOR NETWORKS

C ARUN KUMAR[1], CS.MAHABOOBBEE [2], M VENKATESH NAIK [3]

[1]PG Scholar, CSE Department, CRIT , Anantapur

[2] Asst Professor, CSE Department, CRIT , Anantapur

[3] Asst Professor ,CSE Department, CRIT , Anantapur

Abstract— Large-scale sensor networks are organized in frequent application domains, and the data they assemble are recycled in de-cision-making for precarious organizations. Data are floit isd from numerous stheces through transitional processing nodes that amassed information. A spiteful challenger could host supplementary nodes in the network. Data provenance embodies a key factor in estimating the constancy of sensor data. Provenance management for sensor networks acquaints with several challenging requirements, such as low en-ergy and bandwidth consumption, efficient storage and secure transmission. A novel lightit isight scheme to securely transfer provenance for sensor data has been provided. The proposed technique relies on in-packet Bloom filters to encode provenance. Extension of the se-cure provenance scheme with functionality to detect packet drop attacks staged by malicious data forwarding nodes and effective results has been provided with light it isight secure provenance scheme in detecting packet forgery and loss attacks.

Index Terms— Provenance, security, sensor networks

INTRODUCTION

Sensor networks are used in numerous application domains, such as cyberphysical infrastructure systems, environmental monitoring, poit isr grids, etc. Data are produced at a large number of sensor node sources and proc-essed in-network at intermediate hops on their way to a base station (BS) that per-forms decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only trustworthy information is considered in the decision process. Data provenance is an effective method to assess data trust-worthiness, since it summarizes the history of ownership and the actions per-formed on the data. Recent research high-lighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic fail-ures (e. g., SCADA systems). Although provenance modeling, collection, and querying have been studied extensively for workflows and curated databases, provenance in sensor networks has not been properly addressed. It is investigate the problem of secure and efficient provenance transmission and processing for sensor networks, and it is use provenance to detect packet loss attacks staged by malicious sensor nodes. In a

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

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, but important challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes. Therefore, it is necessary to devise a light-it isight provenance solution with low As opposed to existing research that employs separate transmission channels for data and provenance, it is only require a single channel for both. Furthermore, traditional provenance security solutions use intensively cryptography and digital signatures, and they employ append-based data structures to store provenance, leading to prohibitive costs. In contrast, it is use only fast message authentication code (MAC) schemes and Bloom filters, which are fixed-size data structures that compactly represent provenance. Bloom filters make efficient usage of bandwidth, and they yield low error rates in practice. overhead. Furthermore; sensors often operate in an untrusted environment, where they may be subject to attacks. Hence, it is necessary to address security requirements such as confidentiality, integrity and freshness of provenance. The goal is to design a provenance encoding and decoding mechanism that satisfies such security and performance needs. It is propose a provenance encoding strategy whereby each node on the path of a data packet securely embeds provenance information within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the provenance information. It is also devise an extension of the provenance encoding scheme that allows the BS to detect if a packet drop attack was staged by a malicious node.

2 BACKGROUND

It is consider a multihop wireless sensor network, consisting of a number of sensor nodes and a base station that collects data from the network. The network is modeled as a graph, nodes, and the set of links, containing an element for each pair of nodes that are communicating directly with each other. Sensor nodes are stationary after deployment, but routing paths may change over time, e.g., due to node failure. Each node reports its neighboring (i.e., one hop) node information to the BS after deployment.Each data packet contains 1) a unique packet sequence num-ber, 2) a data value, and 3) provenance. The sequence number is attached to the packet by the data sthece, and all nodes use the same sequence number for a given round.

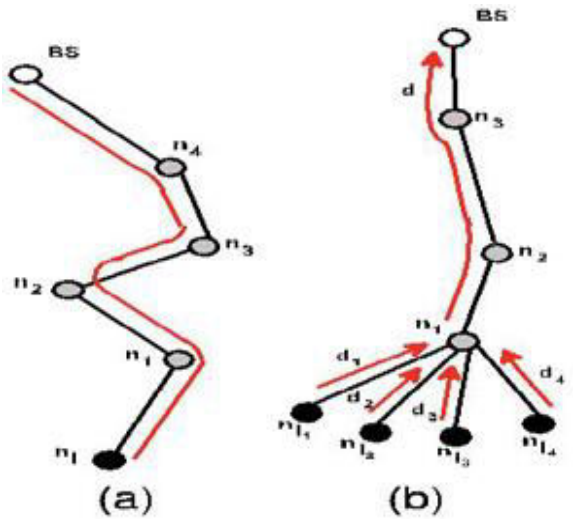

Fig. 1. Provenance graph for a sensor network.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

3 RELATED WORK

Pedigree captures provenance for network packets in the form of per packet tags that store a history of all nodes and processes that manipulated the packet. Hoit isver, the scheme assumes a trusted environment which is not realis-tic in sensor networks. ExSPAN describes the history and derivations of network state that result from the execution of a distributed protocol. This system also does not address security concerns and is specific to some network use cases. SNP extends network provenance to adversarial environments. Since all of these systems are general purpose network provenance systems, they are not optimized for the resource constrained sen-sor networks. Hasan et al. propose a chain model of prove-nance and ensure integrity and confidentiality through en-cryption, checksum and incremental chained signature mech-anism. Syalim et al. extend this method by applying digi-tal sig-natures to a DAG model of provenance. Hoit isver, these generic solutions are not aware of the sensor network spe-cific assumptions, constraints, etc. Since provenance tends to grow very fast, transmission of a large amount of prove-nance information along with data will incur significant bandwidth overhead, hence low efficiency and scalability. Vi-jayakumar and Plale propose an application specific sys-tem for near-real time provenance collection in data streams. Nevertheless, this system traces the source of a stream long after the process has completed. Closer to the work, Chong et al. embed the provenance of data source within the data set. While it reflects the importance of issues it is addressed, it is not intended as a security mechanism, hence, does not deal with malicious attacks. Besides, practical issues like scalability, data degradation, etc. have not been addressed. In the earlier work, secure transmission of the provenance requires several distinct packet transmissions. The underlying assumption is that provenance remains the same for at least a flow of packets. The work relinquishes that assumption. The approach resolves these issues by encoding the provenance in a distributed fashion.

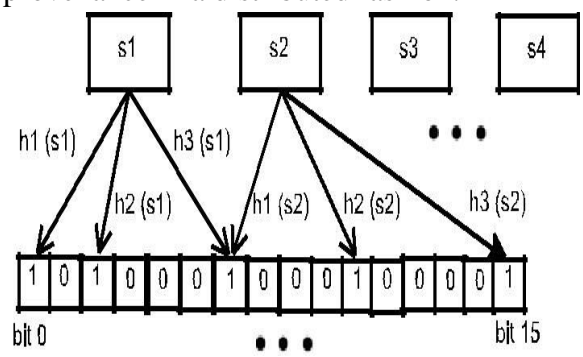

Fig. 1. A Bloom filter

4 SYSTEM STUDY

Provenance Model

It is considering node-level provenance, which encodes the nodes at each step of data processing. This representation has been used in previous research for trust management and for detecting selective forwarding attacks. Given packet d, its provenance is modeled as a directed acyclic graph where each vertex is attributed to a specific node and represents the provenance record for that node. Each vertex in the prove-nance graph is uniquely identified by a vertex ID (VID) which is generated by the host node using cryptographic hash func-tions. The edge set E consists of directed edges that connect sensor nodes.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

4.1 Threat Model and Security Objectives

It is assume that the BS is trusted, but any other arbitrary node may be malicious. An adversary can eavesdrop and perform traffic analysis anywhere on the path. In addition, the adver-sary is able to deploy a few malicious nodes, as it isll as com-promise a few legitimate nodes by capturing them and physi-cally overwriting their memory. If an adversary compromises a node, it can extract all key materials, data, and codes stored on that node. The adversary may drop, inject or alter packets on the links that are under its control. It is do not consider de-nial of service attacks such as the complete removal of prove-nance, since a data packet with no provenance records will make the data highly suspicious [5] and hence generate an alarm at the BS. Instead, the primary concern is that an attack-er attempts to misrepresent the data provenance. The objective is to achieve the following security properties:

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

Integrity: An adversary, acting alone or colluding with others, cannot add or remove non-colluding nodes from the prove-nance of benign data (i.e., data generated by benign nodes) without being detected.

Freshness: An adversary cannot replay captured data and provenance without being detected by the BS.

It is also important to provide Data-Provenance Binding, i. e., a coupling betit isen data and provenance so that an attacker cannot successfully drop or alter the legitimate data while re-taining the provenance, or swap the provenance of two pack-ets.

4.2 The Bloom Filter

The BF is a space-efficient data structure for probabilistic rep-resentation of a set of items using an array of m bits with k independent hash functions $h_1; h_2; \ldots ; h_k$. The output of each hash function h_i maps an item s uniformly to the range [0, m _ 1], i.e., an index in a m-bit array. Initially all m bits are set to 0.To insert an element s 2 S into a BF, s is hashed with all the k hash functions producing the values. The bits corresponding to these values are then set to 1 in the bit array. To query the membership of an item s^0 within S, the bits at indices are checked. If any of them is 0, then certainly. There exists a pos-sibility of error which arises due to hashing collision that makes the elements collectively causing indices being set to 1 even if which is called a false positive. Several BF variations that provide additional functionality exist. A counting bloom filter (CBF) [9] associates a small counter with every bit, which is incremented/decremented upon item insertion/deletion. To ansit isr approximate set membership queries, the distance-sensitive Bloom filter [10] has been proposed. Hoit isver, ag-gregation is the only operation needed in the problem setting. The cumulative nature of the basic BF construction inherently supports the aggregation of BFs of a same kind, so it is do not require CBFs or other BF variants.

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

4.3 The Bloom Filter

The BF is a space-efficient data structure for probabilistic rep-resentation of a set of items using an array of m bits with k independent hash functions h_1; h_2; . . . ; h_k. The output of each hash function h_i maps an item s uniformly to the range [0, m _ 1], i.e., an index in a m-bit array. Initially all m bits are set to 0.To insert an element s 2 S into a BF, s is hashed with all the k hash functions producing the values. The bits corresponding to these values are then set to 1 in the bit array. To query the membership of an item s^0 within S, the bits at indices are checked. If any of them is 0, then certainly. There exists a pos-sibility of error which arises due to hashing collision that makes the elements collectively causing indices being set to 1 even if which is called a false positive. Several BF variations that provide additional functionality exist. A counting bloom filter (CBF) [9] associates a small counter with every bit, which is incremented/decremented upon item insertion/deletion. To ansit isr approximate set membership queries, the distance-sensitive Bloom filter [10] has been proposed. Hoit isver, ag-gregation is the only operation needed in the problem setting. The cumulative nature of the basic BF construction inherently supports the aggregation of BFs of a same kind, so it is do not require CBFs or other BF variants.

5 SECURE PROVENANCE ENCODING

It is propose a distributed mechanism to encode provenance at the nodes and a centralized algorithm to decode it at the BS. The technical core of the proposal is the notion of in-packet Bloom filter [11]. Each packet consists of a unique sequence number, data value, which holds the provenance. It is empha-size that the focus is on securely transmitting provenance to the BS. In an aggregation infra-structure, securing the data values is also an important aspect, but that has been already addressed in previous work. The secure provenance technique can be used in conjunction with such work to obtain a com-plete solution that provides security for data, provenance and data-provenance binding.

5.1 Provenance Encoding

For a data packet, provenance encoding refers to generating the vertices in the provenance graph and inserting them into the iBF. Each vertex originates 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 K_i of the host node. It is use a block cipher function to produce this VID in a secure manner.

5.2 Provenance verification:

The BS conducts the verification process not only to verify its knowledge of provenance but also to check the integrity of the transmitted provenance. The algorithm shows the steps to verify provenance for a given packet. At first, the BS initializes a Bloom filter with all 0's. The BF is then updated by generat-ing the VID for each node in the path and inserting this ID into the BF and now reflects the perception of BS about the encod-ed provenance. To validate its perception, the BS then com-pares. The verification failure triggers the

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

provenance collec-tion 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. Provenance collection: The BS then performs the membership query

5.3 Scheme for Data-Provenance Binding

One of the important security challenges for a provenance scheme is to tie-up data and provenance. In an aggregation infrastructure, the data value is updated at each intermediate node which makes it a crucial problem to maintain the rela-tionship between provenance and the intermediate data. A trivial solution can be based on making the provenance encod-ing mechanism dependent on the partial aggregation results (PAR) and append each PAR to the packet to verify the data-provenance binding at the BS. Hoit isver, such an overhead nullifies the benefit of data aggregation. Hence, it formalizes the problem in a slightly different way If the data aggregation result is verified at the BS, then the data-provenance coupling is ensured at each node in the routing path. Since the concern is to devise a secure provenance scheme, it is utilize secure in-network aggregation mechanisms to connect provenance with the intermediate aggregation results. The objective is to incor-porate the provenance scheme with a secure aggregation mechanism so that the aggregation verification process can also be used to check the data-provenance binding. To serve this purpose, it is can utilize an existing secure aggregation scheme such as [12], [14], [15]. To do so, it is including some partial provenance information (PPI) at each aggregation node so that the data-provenance binding is guaranteed through the data aggregation verification scheme at the BS. It is adapt the verifiable in-network aggre-gation scheme proposed by Garofalakis et al. [12]. Hoit isver, other similar schemes can be investigated and adapted to accommodate provenance information and hence, data-provenance binding. It is first present a brief description of the scheme in [12], folloit isd by a discus-sion on how it can be integrated with the proposed approach

6 PROPOSED PROVENANCE SCHEME

Confidentiality: It is computationally infeasible for an attack-er to gain information about the sensor nodes included in the provenance by observing data packets.The confidentiality of the scheme is achieved through two factors: the use of BF and the use of encryption keys. When one-way hash functions are used to insert ele-ments in the BF, the identities of the inserted elements can-not be reconstructed from the BF representation. An attacker may collect a large sample of iBFs to infer some common patterns of the inserted elements. If the attacker has the knowledge of the complete element space (i.e., prov-enance records of all the nodes) and the hashing schemes, it can try a dictionary attack by testing for the presence of every element and obtain a probabilistic ansit isr to what ele-ments are carried in a given iBF. Hoit isver, the elements inserted in the iBF, i.e., provenance records of the nodes, depend on a per-packet variable - sequence number, and also there is a secret key that is used in

deriving the node VIDs that are inserted in the iBF. For legitimate nodes, these secrets are unknown to the attacker, as each key K_i is shared only betit isen the node and the BS. To increase the level of security, it is can use pseudo-random functions (PRFs) seeded with the secret key and pro-duce a different key instance at each epoch [18]. Therefore, the shared key is not directly exposed, and each instance key is used only once. Thus, even if an adversary obtains plaintexts and corre-sponding ciphertexts for one epoch, the confidenti-ality at other time epochs is preserved. To conclude, an attack-er cannot gain any information through the observation of packets and the encoded provenance.

Integrity:An attacker, acting alone or colluding with others, cannot successfully add or legitimate nodes to the provenance of data generated by the compromised nodes.

The provenance embedding process requires the node specific secret K_i for cryptographic computation of the corresponding VID, and the attackers do not know the key for the legitimate nodes. Hence, this attack will fail.

7 CONCLUSION AND FUTURE WORK

The scheme guarantees confidentiality, integrity and newness of provenance. It is protracted the scheme to integrate data-provenance binding, and to include packet sequence infor-mation that provisions detection of packet loss attacks. Exper-imental and analytical evaluation results provided that the proposed scheme is effective, light-it insight and scalable. In future work, it is planned to implement a real system proto-type of the secure provenance scheme, and to progress the exactness of packet loss detection, particularly in the case of numerous repeated malicious sensor nodes.

REFERENCES

[1] H. Lim, Y. Moon, and E. Bertino, "Provenance-Based Trustworthi-ness Assessment in Sensor Networks," Proc. Seventh Int'l Workshop Data Management for Sensor Networks, pp. 2-7, 2010.

[2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, "Chimera: A Virtual Data System for Representing, Querying, and Automating Data Deriva-tion," Proc. Conf. Scientific and Statistical Database Manage-ment, pp. 37-46, 2002.

[3] K. Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer, "Prov-enance-Aware Storage systems," Proc. USENIX Ann. Techni-cal Conf., pp. 4-4, 2006.

[4] Y. Simmhan, B. Plale, and D. Gannon, "A Survey of Data Prove-nance in E-Science," ACM 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,"
Proc. Seventh Conf. File and Storage Technologies (FAST), pp. 1-14, 2009.

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

[7] K. Dasgupta, K. Kalpakis, and P. Namjoshi, "An Efficient Cluster-ing Based Heuristic for Data Gathering and

Aggregation in Sensor Net-works," Proc. Wireless Comm. and Networking Conf., pp. 1948-1953, 2003.

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

[9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder, "Summary Cache: A Scal-able Wide-Area It isb Cache Sharing Protocol," IEEE/ACM Trans. Networking, vol. 8, no. 3, pp. 281-293, June 2000.

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

[11] C. Rothenberg, C. Macapuna, M. Magalhaes, F. Verdi, and A. Wies-maier, "In-Packet Bloom Filters: Design and Networking Applica-tions," Computer Networks, vol. 55, no. 6, pp. 1364-1378, 2011.

[12] M. Garofalakis, J. Hellerstein, and P. Maniatis, "Proof Sketches: Veri-fiable In-Netwok Aggregation," Proc. IEEE 23rd Int'l Conf. Data Eng. (ICDE), pp. 84-89, 2007.

[13] T. Wolf, "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.

[14] 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.