A Lightweight Secure Scheme for Detecting Provenance Forgery and Packet Drop Attacks in Wireless Sensor Networks

Mrs.K.Valarmathi[1] Mrs.R.Navamani[2] J.Baby[3]
[1]Head of Dept. [2]Assistant Professor
[1,2,3]Department of Computer Science
[1,2,3]Trinity College for Women, Namakkal

Abstract— The frequent application is invented to work in Large-scale sensor network domains. The data composed from wireless sensor network are used in making decision in serious infrastructures. Data’s are originating from many sources and transmit through intermediate meting out nodes. Those nodes achieve the aggregation on information. Attacker concessions those type of networks by introduce 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 origin is an important factor. The several challenging requirements for provenance management in sensor networks are low force and low bandwidth consumption, competent storage space and secure transmission. This survey proposes a new lightweight scheme in order to securely transmit provenance with sensor data. The future in-packet Bloom filters techniques used to program provenance with the sensor data. These mechanisms initially perform origin at the base station then perform rebuilding of the data at the base station. In addition to this the ascription scheme functionality used to detect packet drop attacks prepared by malicious data forwarding nodes. These examinations describe the success and efficiency of the Light weight secure provenance scheme in detect packet forgery with packet loss attacks.

Key words: Sensor Nodes, Forgery

I. Introduction

Data are twisted at a large number of sensor node sources and processed in network at intermediate hops on their way to a base station (BS) that perform decision-making. The diversity of data sources creates the need to assure the trustworthiness of data, such that only dependable information is considered in the decision process. Data provenance is an effective method to assess data dependability, since it summarizes the history of ownership and the actions performed on the data. Recent research, tinted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures. Although provenance modeling, collection, and querying have been studied extensively for effort flow and curated databases, provenance in sensor networks has not been properly addressed. It investigates the predicament of safe and sound and proficient provenance transmission and processing for sensor networks, and we use attribution to detect packet loss attacks dramatic with malicious sensor nodes. In a multi-hop sensor network, data attribution allows the BS to trace the starting place and forwarding path of an individual data packet. Provenance must be record for each packet, but imperative challenges arise due to the tight storage, energy and bandwidth constraints of sensor nodes. Therefore, it is required to devise a light-weight attribution solution with low overhead. In addition, sensors often operate in an untrusted atmosphere, where they may be subject matter to attacks. Hence, it is necessary to address security requirements such as privacy, integrity and freshness of provenance. The purpose is to design an origin encoding and decoding mechanism that satisfies such safety measures and performance needs. It propose a attribution encoding strategy whereby every one node on the path of a data carton securely embeds provenance in order within a Bloom filter (BF) that is transmitted along with the data. Upon receiving the packet, the BS extracts and verifies the attribution information. It also devise an lean-to of the attribution encoding method that allows the BS to detect if a package drop attack was staged by a malicious node.

A. Objective

1) Decrease energy consumption compared to other system.
2) Create a lesser amount of memory usage.
3) Analysis, detection and recovery from the malicious node in wireless network.

II. Related Works

Some of the recent and most relevant works are summarized below: [1] Recent research H. Lim, Y. Moon, and E. Bertino highlighted the key contribution of provenance in systems where the use of untrustworthy data may lead to catastrophic failures (e.g., SCADA systems).Large number of application areas, like location based services, transaction logs, sensor networks is qualified by uninterrupted data stream from many. Chasing of data provenance in extremely active circumstance is a crucial requirement, because data provenance is a key component in appraising data trustiness which is important for lots of application. Provenance handling of continuous data needs to cover various issues, admitting the storage efficiency, processing throughput, bandwidth conception and secure transmission. [2] I. Foster, J. Vockler, M. Wilde, and Y. Zhao, gives information about provenance modeling, collection, and querying and shows studies extensively for workflows and curated databases. The Swift parallel scripting language allows for the speciation, execution and analysis of large-scale computations in parallel and distributed environments. It incorporates a data model for recording and querying provenance information. In this article it describes these capabilities and evaluates interoperability with other systems through the use of the Open Provenance Model. It describe Swift's provenance data model and compare it to the Open Provenance Model. It also describe and evaluate activities performed within the Third Provenance Challenge, which consisted of implementing a specific scientific workow, capturing and recording provenance information of its execution, performing provenance queries, and exchanging provenance information with other system. K.

Muniswamy-Reddy, D. Holland, U. Braun, and M. Seltzer [3], gave the basic terminologies used in provenance record in sensor networks Sensor network data has both historical and real-time value. Making historical sensor data useful, in particular, requires storage, naming, and indexing. Sensor data presents new challenges in these areas. Such data is location-specific but also distributed; it is collected in a particular physical location and may be most useful there, but it has additional value when combined with other sensor data collections in a larger distributed system. Thus, arranging location-sensitive peer-to peer storage is one challenge. Sensor data sets do not have obvious names, so naming them in a globally useful fashion is another challenge. The last challenge arises from the need to index these sensor data sets to make them searchable. The key to sensor data identity is provenance, the full history or lineage of the data. [4] Y. Simmhan, B. Plale, and D. Gannon showed that the emploment of separate transmission channels for data and provenance methology. Current provenance collection systems typically gather metadata on remote hosts and submit it to a central server. In contrast, several data-intensive scientific applications require a decentralized architecture in which each host maintains an authoritative local repository of the provenance metadata gathered on that host. The latter approach allows the system to handle the large amounts of metadata generated when auditing occurs at fine granularity, and allows users to retain control over their provenance records. The decentralized architecture, however, increases the complexity of auditing, tracking, and querying distributed provenance. We describe a system for capturing data provenance in distributed applications, and the use of provenance sketches to optimize subsequent data provenance queries. Experiments with data gathered from distributed workflow applications demonstrate the feasibility of a decentralized provenance management system and improvements in the Efficiency of provenance queries.

Traditional provenance security solutions use intensively cryptography and digital signatures and they employ append-based data structures to store provenance, leading to prohibitive costs. With no provenance records will make the data highly suspicious and hence generate an alarm at the BS The proposed technique do not consider denial of service attacks such as the complete removal of provenance, since a data packet with no provenance records will make the data highly suspicious Nevertheless, this system traces the source of a stream long after the process has completed. Hasanet al propose a chain model of provenance and ensure integrity and confidentiality through encryption, checksum and incremental chained signature mechanism.

S. Madden, J. Franklin, J. Hellerstein, and W. Hong assume a multiple-round process of data collection. Each sensor generates data periodically, and individual values are aggregated towards the BS using any existing hierarchical (i.e., tree-based) dissemination scheme. Present the Tiny Aggregation (TAG) service for aggregation in low-power, distributed, wireless environments. TAG allows users to express simple, declarative queries and have them distributed and executed efficiently in networks of low-power, wireless sensors. It discusses various generic properties of aggregates, and show how those properties affect the performance of our in network approach. It includes a performance study demonstrating the advantages of our approach over traditional centralized, out-of-network methods, and discusses a variety of optimizations for improving the performance and fault-tolerance of the basic solution. [7] K. Dasgupta, K. Kalpakis, and P. Namjoshi showed how the sequence number is attached to the packet by the data source, and all nodes use the same sequence number for a given round. Energy is one of the most important items to determine the network lifetime due to low power energy nodes included in the network. Generally, data aggregation tree concept is used to find an energy efficient solution. However, even the best aggregation tree does not share the load of data packets to the transmitting nodes fairly while it is consuming the lowest possible energy of the network. Therefore, after some rounds, this problem causes to consume the whole energy of some heavily loaded nodes and hence results in with the death of the network. In this paper, by using the Genetic Algorithm (GA), we investigate the energy efficient data collecting spanning trees to find a suitable route which balances the data load throughout the network and thus balances the residual energy in the network in addition to consuming totally low power of the network. Using an algorithm which is able to balance the residual energy among the nodes can help the network to withstand more and consequently extend its own lifetime. [8] S. Sultana, E. Bertino, and M. Shehab showed the detail concept of distributed computing environment. the use of bloom filters in the distributed systems for provenance detection and its use. Malicious packet dropping attack is a major security threat to the data traffic in the sensor network, since it reduces the legal network throughput and may hinder the propagation of sensitive data. Dealing with this attack is challenging since the unreliable wireless communication feature and resource constraints of the sensor network may cause communication failure and mislead to the incorrect decision about the presence of such attack. [9] L. Fan, P. Cao, J. Almeida, and A.Z. Broder introduces a counting bloom filter (CBF) associates a small counter with every bit, which is incremented/decremented Upon item insertion/deletion. Study the set reconciliation problem, in which each member of a node pair has a set of objects and seeks to deliver its unique objects to the other member. How could each node compute the set difference, however, is challenging in the set reconciliation problem. To address such an issue, we propose a lightweight but efficient method that only requires the pair of nodes to represent objects using a counting Bloom filter (CBF) of size $(O(d))$ and exchange with each other, where (d) denotes the total size of the set differences. A receiving node then subtracts the received CBF from its local one via minus operation proposed in this paper. The resultant CBF can approximately represent the union of the set differences and thus the set difference to each node can be identified after querying the resultant CBF.

A. Kirsch and M. Mitzenmacher answers the approximate set membership queries, the distance sensitive Bloom filter has been proposed by them. Transactional Memory (TM) is an alternative to conventional multithreaded programming to ease the writing of concurrent programs. In the context of unbounded TM, concurrent threads may use hardware signatures to record all the memory addresses issued inside a transaction to detect conflicts. Signatures are usually implemented as perth read fixed hardware Bloom filters that summarize a very large amount of read and write memory addresses at the cost of false conflicts (detection of non-existing conflicts). In this paper, to reduce the probability of false conflicts, a novel signature design that exploits spatial locality is proposed. The design is based on new hash function mappings, so that nearby located addresses share some bits inserted in the filters. This is favorable particularly for large transactions that usually exhibit some amount of spatial locality. Besides, its implementation does not require extra hardware.

III. Existing System

This review state 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 pack Provenance must be recorded but there is an important face arises due to the important storage, energy and bandwidth conditions of sensor nodes. So, it is necessary to provide a light-weight provenance socheme with low overhead.

A. *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.

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.

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.

B. *Disadvantage*

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

IV. The Proposed System

The aim is to plan a provenance encoding and decoding mechanism which satisfy 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

- Make the trouble of secure provenance transmission in sensor networks, and identify the challenges specific tot this context.

1) Design an effective technique for provenance decoding and verification at the base station.
2) expand the secure provenance encoding scheme and devise a mechanism that detects packet drop attacks staged by malicious forwarding sensor nodes.
3) Complete a detailed security analysis and performance evaluation of the proposed provenance encoding scheme and packet loss detection mechanism.

A. *Advantages of Proposed System*

- The high-speed 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.

V. CONCLUSIONS

These examinations address the problem of how firmly transmit provenance for sensor networks. Based on Bloom filters this term paper planned a light-weight provenance encoding and decoding scheme. The method ensures discretion, integrity and freshness of provenance. Also this scheme extended to incorporate data-provenance joining, and to include packet string information that supports detection of packet loss attacks. The proposed scheme is measured as effective, light-weight and scalable. This survey plan gear a real system sample of secure provenance scheme, and to enlarge the truth of packet loss detection, more than ever in the case of multiple never-ending malicious sensor nodes.

REFERENCES

[1] Andreas Merentitis, Nektarios Kranitis,Antonis Paschalis and Dimitris Gizopoulos,”Low Energy Online SelfTest of Embedded Processors in Dependable WSN Nodes” IEEE transactions on dependable and secure computing, vol. 9, no. 1, january/February 2012,pp.86-100.

[2] Charalampos Konstantopoulos, Grammati Pantziou, Damianos Gavalas,Aristides Mpitziopoulos, and Basilis Mamalis,”A Sensor-Based Approach Enabling Energy-Efficient Sensory Data Collection with le Sinks” IEEE transactions on parallel and distributed systems, vol. 23, no. 5, May 2012, pp.809-817.

[3] Degan Zhang,Guang Li,Ke Zhen, Xuechao Ming and Zhao-Hua Pan,” An Energy-Balanced Routing Method Based on Forward-Aware Factor for Wireless Sensor Networks” IEEE transactions on industrial informatics, vol. 10, no. 1, february 2014,pp.766-773.

[4] Guoliang Xing,Tian Wang, Zhihui Xie, and Weijia Jia,”Sensor Planning in Wireless Sensor Networks with le Elements” IEEE transactions on le computing, vol. 7, no. 12, Dec 2008, pp.1430-1443.

[5] Hana Besbes, George Smart,Dujdow Buranapanichkit,Christos Kloukinas, and Yiannis Andreopoulos,” Analytic Conditions for Energy Neutrality in Uniformly-Formed Wireless Sensor Networks” IEEE transactions on wireless communications, vol. 12, no. 10, October 2013,pp.4916-4931.

[6] Issa M. Khalil,”ELMO: Energy Aware Local Monitoring in Sensor Networks” IEEE transactions on dependable and secure computing, vol. 8, no. 4, july /august 2011, pp.523-536.

[7] Jiajia Liu, Xiaohong Jiang, Hiroki Nishiyama and Nei Kato,” On the Delivery Probability of Two-Hop Relay MANETs with Erasure Coding” IEEE transactions on communications, vol. 61, no. 4, April 2013, pp.1314-1326.

[8] Kashif Saleem, Norsheila Fisal and Jalal Al-Muhtadi,” Empirical Studies of BioInspired Self-Organized Secure Autonomous Routing Protocol” IEEE sensors jouSNal, vol. 14, no. 7, july 2014, pp.2232-2239.

[9] Ljubica Blazevic, Jean-Yves Le Boudec and Silvia Giordano, “A Location-Based Routing Method for le Ad Hoc Networks” IEEE transactions on le computing, vol. 3, no. 4, October-December 2004, pp.1-15.

[10] Marios Gatzianas and Leonidas Georgiadis, ”A Distributed Algorithm for Maximum Lifetime Routing in Sensor Networks with le Sink” IEEE transactions on wireless communications, vol. 7, no. 3, March 2008, pp.984-994.

[11] Oualid Demigha, Walid-Khaled Hidouci, and Toufik Ahmed,” On Energy Efficiency in Collaborative Target Tracking in Wireless Sensor Network: A Review” IEEE communications surveys & tutorials, vol. 15, no. 3, third quarter 2013,pp.1210-1222.

[12] Özgür B. Akan,and Ian F. Akyildiz,” Event-to-NodeReliable Transport in Wireless Sensor Networks” IEEE/ACM transactions on networking, vol. 13, no. . 5, october 2005,pp.1003-1016.