International Journal of Research
Available at https://edupediapublications.org/journals

p-ISSN: 2348-6848
e-ISSN: 2348-795X
Volume 04 Issue 07
June 2017

Detecting Packet Drop and Forgery Attacks in Wireless Sensor Networks

[1] B.Charishma,[2] P.Srinivas Rao, [3] M.Narender
[1]M.Tech ,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India
[2]Associate professor,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India
[3]Assistant professor,CSE, Jayamukhi Institute Of Technological Sciences,Warangal,India

Abstract:

The frequent application is fictitious to work in Large-scale sensing element network domains, and also the knowledge they assemble are recycled in decision-making for precarious organizations. Data’s are originating from varied sources and transmit through transformation process nodes that congregate data. Those nodes bring home the bacon the aggregation on data. A vindictive contestant might host supplementary nodes within 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 energy and bandwidth consumption, efficient storage 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. Additionally to the present the ascription theme practicality wont to observe packet drop attacks ready by malicious knowledge forwarding nodes. These examinations describe the success and potency of the light weight secure provenance theme in observes packet forgery with packet loss attacks.

Keywords: Provenance, security, sensor networks

I. Introduction:

Sensor networks area unit employed in various application domains, like cyberphysical infrastructure systems, environmental watching, grids, etc. Data are produced at an oversized variety of detector node sources and processed in network at intermediate hops on their thanks to a base station (BS) that performs decision-making. The range of information sources creates the necessity to assure the trustiness of information, specified solely trustworthy data is taken into account within the call method. knowledge provenance is a good technique to assess knowledge trust-worthiness, since it summarizes the history of possession and therefore the actions per-formed on the information. Recent analysis [1] high-lighted the key contribution of provenance in systems wherever the utilization of teflon knowledge could cause harmful failures (e. g., SCADA systems). Though provenance modeling, collection, and querying are studied extensively for workflows and curated databases [2], [3], provenance in sen-sor networks has not been properly addressed . it's investigate the matter of secure and economical provenance transmission and process for detector networks, and it's use provenance to discover packet loss attacks staged by malicious detector nodes.In a multi-hop detector network, knowledge provenance permits the BS to trace the sourceand forwarding path of a private knowledge packet. provenance should be recorded for every packet, however vital challenges arise attributable to the tight storage, energy and information measure constraints of detector nodes. Therefore, it's necessary to plan a light-it isight provenance resolution with low As against existing analysis that employs separate transmission channels for knowledge and provenance [4], it's solely need one channel for each. what is more, ancient provenance security solutions use intensively cryptography and digital signatures [5], and that they use append-based knowledge structures to store provenance, resulting in preventative prices. In distinction, it's use solely quick message authentication code (MAC) schemes and Bloom filters, that area unit fixed-size knowledge structures that succinctly represent provenance. Bloom filters create economical usage of information measure, and that they yield low error rates in follow. overhead. Furthermore; sensors typically operate in associate untrusted atmosphere, wherever they'll be subject to attacks. Hence, it's necessary to deal with security necessities like confidentiality, integrity and freshness of provenance. The goal is to style a provenance secret writing and decryption mechanism that satisfies such security and performance wants. it's propose a provenance secret writing strategy whereby every node on the trail of data packet firmly embeds provenance information at intervals a Bloom filter (BF) that's transmitted alongside the information. Upon receiving the packet, the BS extracts and verifies the provenance data. it's conjointly devise associate extension of the provenance secret writing theme that enables the BS to discover if a packet drop attack was staged by a malicious node.

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. System Work:

The aim is to set up a source cryptography and secret writing mechanism that satisfy security and performance wants. It proposes a source cryptography strategy in this every node on the trail of a knowledge packet firmly embeds source information inside a Bloom filter (BF) ought to be transmitted together with the info. whereas receiving the packet the bottom Station extracts and verifies the source info. The extension of the source cryptography theme permits the bachelor's degree to notice packet drop attack organized by a malicious node. The options area unit makes the difficulty of secure source transmission in device networks, and establish the challenges specific tot this context. style an efficient technique for source secret writing and verification at the bottom station. Expand the secure source cryptography theme and devise a mechanism that detects packet drop attacks staged by malicious forwarding device nodes. Complete an in depth security analysis and performance analysis of the projected source cryptography theme and packet loss detection mechanism. The high-speed message authentication code (MAC) schemes and Bloom filters area unit fixed-size knowledge structures that with efficiency represent source. Bloom filters build economical usage of information measure, and that they yield low error rates Claim for Confidentiality is computationally unfeasible to Associate in Nursing wrongdoer to achieve knowledge regarding the device nodes enclosed within the source. Associate in Nursing wrongdoer, acting as single user or colluding with others within the cluster cannot with success add or legitimate nodes to the info generated by the compromised/already attack happened nodes. Associate in Nursing wrongdoer or a collection of cooperative attackers cannot by selection add or take away nodes from the source of knowledge generated by legitimate nodes

IV. Conclusion:

These examinations address the matter of however firmly transmit source for device networks. supported Bloom filters this schoolwork planned a light-weight source encryption and cryptography theme. the tactic ensures discretion, integrity and freshness of source. conjointly this theme extended to include data-provenance connexion, and to incorporate packet string info that supports detection of packet loss attacks. The planned theme is measured as effective, light-weight and ascendable. This survey arrange gear a true system sample of secure source theme, and to enlarge the reality of packet loss detection, over ever within the case of multiple endless malicious device 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] 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.

[12] 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.

[13] 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.

[14] 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.

[15] 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.

[16] 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.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.